



UNIVERSIDADE FEDERAL DE SERGIPE - UFS
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA - CCET
DEPARTAMENTO DE COMPUTAÇÃO - DCOMP
CAMPUS SÃO CRISTÓVÃO

ALEF MENEZES DOS SANTOS
DANILO GOIS DOS ANJOS

BOAS PRÁTICAS DE GOVERNANÇA DE TIC ADOTADAS PARA A MELHORIA
DO IGOVTI NA APF NA DIMENSÃO DE PROCESSOS

SÃO CRISTÓVÃO - SE
2017



UNIVERSIDADE FEDERAL DE SERGIPE - UFS
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA - CCET
DEPARTAMENTO DE COMPUTAÇÃO - DCOMP
CAMPUS SÃO CRISTÓVÃO

ALEF MENEZES DOS SANTOS
DANILO GOIS DOS ANJOS

BOAS PRÁTICAS DE GOVERNANÇA DE TIC ADOTADAS PARA A MELHORIA
DO IGOVTI NA APF NA DIMENSÃO DE PROCESSOS

Trabalho de Conclusão de Curso apresentado
Departamento de Computação da
Universidade Federal de Sergipe – UFS como
pré-requisito para a obtenção do título de
Bacharel em Sistemas de Informação.

Área de Concentração: Engenharia de
Software

Orientador: Dr. Rogério Patrício Chagas do
Nascimento

Coorientadora: Esp. Marianne Batista Diniz da
Silva

SÃO CRISTÓVÃO - SE
2017

Trabalho de Conclusão de Curso, Sistemas de Informação, apresentado por Alef Menezes dos Santos e Danilo Gois dos Anjos como parte dos requisitos para obtenção do título de Bacharel em Sistemas de Informação outorgado pela Universidade Federal de Sergipe – UFS Campus São Cristóvão – SE.

APROVADO EM: ____/____/____

BANCA EXAMINADORA:

Prof. Rogério Patrício Chagas do Nascimento,
Dr.

Orientador

Prof(a). Marianne Batista Diniz da Silva, Esp.

Coorientadora

Prof. Gilton José Ferreira da Silva, Me.

Membro

Prof(a). Denise Xavier Fortes, Esp.

Membro

Dedicamos este trabalho as nossas amadas
Mães, que sempre estiveram presentes nos
momentos mais difíceis de nossas vidas.

AGRADECIMENTOS

Muitos agradeceriam a Deus em primeiro lugar, mas eu agradeço a minha Mãe, Lizete Menezes. Sem o carinho dela, afirmo com toda certeza do mundo, eu não estaria hoje agradecendo por esta conquista. Ela que foi meu anjo da guarda e base de tudo o que tenho conquistado. Muito, mais muito OBRIGADO por acreditar em mim, minha amada Mãe!

À minha namorada, Lilian Aparecida, por todo o apoio, incentivo, carinho e paciência ao longo dessa jornada, sempre sendo a mais compreensiva de todas e me ajudando sempre que possível. Você também faz parte dessa batalha. Obrigado meu Amor!

Aos meus orientadores, por possibilitar que mais esse objetivo fosse conquistado, obrigado Prof. Dr. Rogério Patrício C. do Nascimento. E a Mãe e Mestre, Marianne B. Diniz da Silva, que foi sim todos esses adjetivos, sendo tão presente, prestativa e AMIGA acima de tudo, tornando o desenvolver desse trabalho tão prazeroso. Muito obrigado, Mãe Marianne!

A minha dupla, Danilo Gois, que foi meu amigo durante toda a graduação e neste árduo trabalho. E, agradeço também ao querido Prof. Me. Gilton José (MAL), oferecendo sua sabedoria e atenção sempre que possível. Obrigado, meu muito obrigado a todos vocês!

Alef Menezes dos Santos

Agradeço a Deus acima de tudo, por ter colocado pessoas maravilhosas em minha caminhada e por sempre iluminar meus passos, até quando por algum motivo duvidei da minha capacidade, Ele estava lá para sempre mostrar o caminho certo.

Aos meus pais, Vania e Joel, em especial a minha mãe por ser sempre essa pessoa maravilhosa, iluminada e gentil. Obrigado por me criar com todos os princípios e caráter que tenho hoje, por ajudar com tudo que estava a seu alcance e sempre me amparar nos momentos de fraqueza.

À minha namorada, Jusimara, por sempre me apoiar e incentivar a persistir nessa caminhada. Obrigado por ser essa pessoa doce e amável, obrigado por fazer minha vida mais alegre e iluminada. Obrigado minha princesa.

Às pessoas que me ajudaram a concluir essa importante etapa da graduação. À minha dupla neste trabalho, meu amigo Alef, aos nossos orientadores Prof. Dr. Rogério Patrício e a Mãe e Mestre, Marianne B. Diniz, sempre serei seu filho número 2, obrigado por toda a orientação sobre o TCC e sobre a vida. E não poderia faltar o nosso querido Prof. Me. Gilton José, por sempre nos orientar nessa jornada. Muito obrigado a todos, vocês são demais.

Danilo Gois dos Anjos

*“Sonhos determinam o que você quer. Ação
determina o que você conquista.”*

(Aldo Novak)

RESUMO

A Governança é um fator essencial para longevidade de uma organização. Logo, ela não é um tema exclusivo às organizações de cunho privado. Portanto, devemos considerar que também se aplica a Administração Pública Federal (APF). Partindo desse princípio, a Governança pode ser aplicada em diversos setores de uma organização, como: os recursos humanos, o financeiro, a alta administração e da Tecnologia da Informação e Comunicação (TIC). Já esse último, é de suma importância para que seja possível alcançar os objetivos organizacionais, alinhando os recursos e objetivos da TIC ao negócio. Segundo o Tribunal de Contas da União (TCU) do Brasil, a grande maioria dos órgãos que compõem a APF têm o índice de maturidade baixo. Portanto, esse trabalho tem como objetivo identificar e apresentar de forma resumida e simplificada as boas práticas de Governança de TIC (GovTIC), de modo a auxiliar os gestores da APF na adoção dessas práticas em sua organização, dentro da dimensão de Processos definido pelo TCU, com a pretensão de elevar o nível de maturidade da organização. Também foi desenvolvido um modelo *Business Process Management* (BPM), levando em consideração as boas práticas identificadas e analisadas, visando à melhoria dos resultados da dimensão de Processos. Esse modelo foi validado por meio de um questionário respondido pelos gestores ou servidores da APF que são responsáveis pela GovTIC em sua organização. E o modelo proposto obteve respostas satisfatórias, o que indica que sua aplicação pode auxiliar os gestores de Tecnologia da Informação (TI) na melhoria da maturidade do Índice de Governança de Tecnologia da Informação (iGovTI) na dimensão de Processos. Além de verificar que o envolvimento da alta administração é de suma importância para que este objetivo seja alcançado.

Palavras-chave: Governança. Administração pública federal. Boas Práticas. TIC. BPM.

ABSTRACT

Governance is an essential factor for the longevity of an organization. Soon, it is not an exclusive theme for private organizations. Therefore, we must consider that the Federal Public Administration (FPA) also applies. Based on this principle, Governance can be applied to several sectors of an organization, such as human resources, finance, high management and Information and Communication Technology (ICT). Already the latter is of paramount importance in order to achieve the organizational objectives, aligning the resources and objectives of the ICT to the business. According to the Court of Audit of the Union (CAU) of Brazil, the great majority of the bodies that compose the APF have a low maturity index. Therefore, this work aims to identify and present in a summarized and simplified form the good practices of ICT Governance, in order to assist FPA managers in the adoption of these practices in their organization, within the Process dimension defined by TCU, with the aim of raising the level of maturity of the organization. Was also developed a Business Process Management (BPM) model, taking into account the good practices identified and analyzed, aiming at improving the results of the process dimension. This model was validated by means of a questionnaire answered by managers or servers of APF that are responsible for ICT Governance in your organization. And the proposed model obtained satisfactory answers, which indicates that its application can assist Information Technology (IT) managers in improving the maturity of the Information Technology Governance Index in the dimension of Process. In addition to verifying that the involvement of top management is of paramount importance in order to achieve this goal.

Keywords: Governance. Federal public administration. Good practices. ICT. BPM.

LISTA DE FIGURAS

Figura 1 - Organizações avaliadas em 2016.	25
Figura 2 - Distribuição de frequência do iGovTI 2016 na APF.	27
Figura 3 - Modelo de visão geral para Implementação das Boas Práticas.	60
Figura 4 - Modelo de Implementação para Gerenciamento de Serviços de TI.	61
Figura 5 - Modelo de Implementação para Gerenciamento de Nível de Serviço de TI.	62
Figura 6 - Modelo de Implementação para Gestão de Risco de TI.	63
Figura 7 - Modelo de Implementação para Gestão Corporativa da Segurança da Informação.	65
Figura 8 - Modelo de Implementação para Processo de <i>Software</i>	66
Figura 9 - Modelo de Implementação para Gerenciamento de Projetos de TI.	67
Figura 10 - Modelo de Implementação para Contratações de Serviços de TI.	68
Figura 11 - Modelo de Implementação para Planejamento das Contratações de TI.	69
Figura 12 - Modelo de Implementação para Gestão dos Contratos de TI.	70
Figura 13 - Resultado da Questão 01.	71
Figura 14 - Resultado das Questões 02, 03, 04, 07 e 08.	72
Figura 15 - Resultado da Questão 05.	72
Figura 16 - Resultado da Questão 06.	73
Figura 17 - Resultado da Questão 09.	74
Figura 18 - Resultado da Questão 10.	74
Figura 19 - Resultado das Questões 11 e 12.	75
Figura 20 - Resultado das Questões 13, 14, 15, 16 e 17.	75

LISTA DE QUADROS

Quadro 1 - Dimensões da TIC.....	26
Quadro 2 - Cálculo do iGovTI.....	27
Quadro 3 - Boas práticas de GovTIC identificadas.	28
Quadro 4 - Comparativo de características dos trabalhos relacionados.....	34
Quadro 5 - Boas práticas para Gerenciamento de Serviços de TI.	38
Quadro 6 - Boas práticas para Gerenciamento de Nível de Serviço de TI.	41
Quadro 7 - Boas práticas para Gestão de Riscos de TI, parte 1.....	42
Quadro 8 - Boas práticas para Gestão de Riscos de TI, parte 2.....	43
Quadro 9 - Boas práticas de Gestão Corporativa da Segurança da Informação, parte 1.	44
Quadro 10 - Boas práticas de Gestão Corporativa da Segurança da Informação, parte 2.	46
Quadro 11 - Boas práticas de Processo de <i>Software</i>	51
Quadro 12 - Boas práticas de Gerenciamento de Projetos de TI.	52
Quadro 13 - Boas práticas para Contratações de Serviços de TI.....	54
Quadro 14 - Boas práticas de Planejamento das Contratações de TI.....	56
Quadro 15 - Boas práticas de Gestão dos Contratos de TI.	56
Quadro 16 - Questões relativas ao Perfil das Contratações de TI.....	57
Quadro 17 - Dicionário de Símbolos BPM utilizando o Bizagi.	59

LISTA DE ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
ANS	Acordo de Nível de Serviço
APF	Administração Pública Federal
APO	<i>Align, Plan and Organize</i>
BAI	<i>Build, Acquire and Implement</i>
BPM	<i>Business Process Management</i>
CAU	<i>Court of Audit of the Union</i>
CMM	<i>Capability Maturity Model</i>
CMMI	<i>Capability Maturity Model - Integration</i>
COBIT	<i>Control Objectives For Information end Related Technology</i>
COSO	<i>Committee of Sponsoring Organizations</i>
EGD	Estratégia de Governança Digital
GovTIC	Governança de Tecnologia da Informação e Comunicação
IBGC	Instituto Brasileiro de Governança Corporativa
ICT	<i>Information and Communication Technology</i>
iGovTI	Índice de Governança de Tecnologia da Informação
IEC	<i>International Electrotechnical Commission</i>
ISACA	<i>Information Systems Audit and Control Association</i>
ISO	<i>International Organization for Standardization</i>
ITIL	<i>Information Technology Infrastructure Library</i>
MAngve	Modelo Ágil no apoio à Governança em TIC
MCTIC	Ministério da Ciência, Tecnologia, Inovações e Comunicações
MPU	Ministério Público da União
NBR	Norma Brasileira
OGC	<i>Office of Government Commerce</i>
PMBOK	<i>Project Management Body of Knowledge</i>
PMI	<i>Project Management Institute</i>
SEI	<i>Software Engineering Institute</i>
SGSI	Sistema de Gerenciamento de Segurança da Informação
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SPICE	<i>Software Process Improvement and Capability dEtermination</i>

STI/MPOG	Secretaria de Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação

SUMÁRIO

1	INTRODUÇÃO	15
1.1	CONTEXTUALIZAÇÃO	15
1.2	PROBLEMÁTICA	16
1.3	OBJETIVOS: GERAL E ESPECÍFICOS	16
1.4	JUSTIFICATIVA	17
1.5	ESTRUTURA DO TRABALHO	17
2	REFERENCIAL TEÓRICO	19
2.1	GOVERNANÇA CORPORATIVA	19
2.2	GOVERNANÇA CORPORATIVA PÚBLICA	20
2.3	GOVERNANÇA DE TIC	21
2.4	GOVERNANÇA DE TIC NA APF BRASILEIRA	22
2.4.1	Sistema de Administração de Recursos de Tecnologia da Informação	22
2.4.2	Secretaria de Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão	23
2.4.3	Estratégia de Governança Digital	23
2.5	AVALIAÇÃO DA GOVERNANÇA DE TIC NA APF DO BRASIL	24
2.5.1	Situação Atual da Governança de TIC no Governo Federal, na Visão do TCU	25
2.6	BOAS PRÁTICAS PARA MELHORIA DA GOVTIC	28
2.7	TRABALHOS RELACIONADOS	32
3	METODOLOGIA	35
3.1	CLASSIFICAÇÃO DA PESQUISA	35
3.2	INSTRUMENTAÇÃO	36
3.2.1	Instrumentação: <i>Business Process Management</i>	36
3.2.2	Instrumentação: Questionário de Verificação e Validação	37
4	ANÁLISE DAS BOAS PRÁTICAS	38
4.1	GERENCIAMENTO DE SERVIÇOS DE TI	38
4.2	GERENCIAMENTO DE NÍVEL DE SERVIÇO DE TI	40
4.3	GESTÃO DE RISCO DE TI	42
4.4	GESTÃO CORPORATIVA DA SEGURANÇA DA INFORMAÇÃO	44
4.5	PROCESSO DE <i>SOFTWARE</i>	50
4.6	GERENCIAMENTO DE PROJETOS DE TI	52
4.7	CONTRATAÇÕES DE SERVIÇOS DE TI	54

4.8	PLANEJAMENTO DAS CONTRATAÇÕES DE TI	55
4.9	GESTÃO DOS CONTRATOS DE TI	56
4.10	PERFIL DAS CONTRATAÇÕES DE TI	57
4.11	VISÃO GERAL	58
5	MODELO DE PROCESSOS DAS BOAS PRÁTICAS	59
5.1	GERENCIAMENTO DE SERVIÇOS DE TI	61
5.2	GERENCIAMENTO DE NÍVEL DE SERVIÇO DE TI	62
5.3	GESTÃO DE RISCO DE TI	63
5.4	GESTÃO CORPORATIVA DA SEGURANÇA DA INFORMAÇÃO	64
5.5	PROCESSO DE <i>SOFTWARE</i>	66
5.6	GERENCIAMENTO DE PROJETOS DE TI	67
5.7	CONTRATAÇÕES DE SERVIÇOS DE TI	68
5.8	PLANEJAMENTO DAS CONTRATAÇÕES DE TI	69
5.9	GESTÃO DOS CONTRATOS DE TI	70
6	RESULTADOS DO QUESTIONÁRIO DE VALIDAÇÃO E VERIFICAÇÃO	71
6.1	RESULTADO DA SEÇÃO 1: MODELOS BPM	71
6.2	RESULTADO DA SEÇÃO 2: ANÁLISE DAS BOAS PRÁTICAS	74
7	CONCLUSÃO	76
7.1	DIFICULDADES E AMEAÇAS A VALIDADE	77
7.2	TRABALHOS FUTUROS	77
7.3	CONTRIBUIÇÕES AO TRABALHO	77
	REFERÊNCIAS BIBLIOGRÁFICAS	78
	APÊNDICES	82
	APÊNDICE A: E-MAIL	82
	APÊNDICE B: QUESTIONÁRIO	83
	ANEXOS	90
	ANEXO A: E-MAIL DE APROVAÇÃO DO ARTIGO	90

1 INTRODUÇÃO

Neste capítulo têm-se a introdução para este trabalho de pesquisa. Na seção 1.1 apresenta-se a contextualização da temática utilizada na pesquisa. Em seguida, na seção 1.2 encontra-se a problemática que motivou o presente trabalho. Na seção 1.3 têm-se o objetivo geral e os específicos a serem alcançados. Logo após, na seção 1.4 têm-se a justificativa para a elaboração deste trabalho. E por fim, na seção 1.5 encontra-se a estrutura definida para este trabalho.

1.1 CONTEXTUALIZAÇÃO

A Governança de Tecnologia da Informação e Comunicação (GovTIC) na Administração Pública Federal (APF) do Brasil, enfrenta um cenário desfavorável, relativo ao baixo investimento nas políticas de GovTIC, conforme TCU (2014, 2017), levando ao aumento do risco de insucesso de projetos, desperdício de recursos, serviços com menor qualidade e entre outros. A adoção de boas práticas pode ser uma maneira de extinguir ou mitigar tais problemáticas.

A Governança Corporativa surge como uma estratégia para dirigir e orientar as organizações a atingir seus objetivos envolvendo os *stakeholders*¹ (adaptado de IBGC, 2015). Entretanto, a governança de modo geral não se restringe às organizações privadas, logo, ela também é utilizada no setor público. A Governança Corporativa Pública é uma síntese dos princípios e práticas voltadas à eficiência, eficácia e efetividade dos resultados para uma boa administração pública (adaptado de BIZERRA; ALVES; RIBEIRO, 2012). A GovTIC é uma forma de governar os recursos de Tecnologia da Informação (TI), a fim de obter o controle e direcionar o uso atual e futuro da Tecnologia da Informação e Comunicação (TIC) dentro da organização (ABNT, 2009c).

Para isso, é necessária uma adesão de boas práticas com intuito de melhoria da GovTIC, visto que sua adesão pode afetar positivamente a sociedade em geral. A gestão da governança de processos pode ser uma solução para minimizar este cenário, dado que a dimensão de Processos de TIC oferece os controles da gestão de processos, sendo alguns

¹ *Stakeholders*: são as partes interessadas (usuários dos serviços, cidadãos, sociedade em geral, alta administração, sócios e todas as pessoas e/ou organizações que possam ser afetadas).

deles: de risco de TI, a corporativa da segurança da informação, de projetos de TI e contratações de serviços de TI, e o monitoramento dos mesmos (TCU, 2017).

1.2 PROBLEMÁTICA

Com base no levantamento realizado pelo Tribunal de Contas da União (TCU) em 2016 e divulgado em 2017, foi constatado que apenas 11% das organizações pertencentes a APF apresenta nível de governança aprimorado, em contrapartida, 51% delas estão nos níveis mais inferiores, sendo que no inicial 14% e no básico 37%. Isto demonstra o baixo nível de governança das organizações da APF, logo dificilmente as TIC irão contribuir de forma efetiva, no sentido de geração de valor ao negócio.

O último levantamento realizado pelo TCU (2017), revela uma situação negativa entre as práticas envolvidas na dimensão de Processos. No que se refere à Gestão de Riscos de TI, os resultados demonstram baixo nível de maturidade e negligencia quanto à sua importância, acarretando perda de prazos de entrega, no custo elevado e na qualidade do produto. Já na Gestão Corporativa da Segurança da Informação foi constatado que o nível de adoção das práticas está muito abaixo do esperado, ocasionando a indisponibilidade de serviços e perda da integridade de informações. No que diz respeito ao Gerenciamento de Projetos de TI, foi identificado que 36% das organizações da APF não realizam um processo de gerenciamento de TI e 55% não possuem um escritório de projetos, situação que leva ao risco de fracasso nos mesmos. No âmbito da Contratação de Serviços de TI, apesar da aparente evolução do seu nível de maturidade, foi identificada a existência de irregularidades na realização de suas contratações. De modo geral, é notável a evolução entre os resultados de 2014 para 2016, porém ainda existem inúmeros pontos passíveis de melhoria.

Diante deste cenário, verifica-se que a gestão ineficiente dos recursos públicos, provoca o desperdício e/ou uso indevido dos recursos destinado aos setores de TI das organizações da APF. Esses recursos tinham como finalidade a prestação de serviços de qualidade a sociedade e a falta da adoção de tais práticas pode ser punida no que prevê o órgão regulador vigente - TCU - com base em competências constitucionais e/ou legais.

1.3 OBJETIVOS: GERAL E ESPECÍFICOS

Esta pesquisa tem como objetivo geral realizar uma análise de qual(is) boa(s) prática(s) adotar em organizações da APF para melhorar a maturidade do Índice de

Governança de Tecnologia da Informação (iGovTI) na dimensão de Processos, conforme definido pelo TCU.

Para atingir o objetivo geral, decorrem-se como necessários os seguintes objetivos específicos:

- a) Foi identificado quais as boas práticas de GovTIC devem ser adotadas em organizações públicas;
- b) Foi criado o processo de implementação, por meio de *Business Process Management* (BPM) das boas práticas a serem adotadas;
- c) Foi realizado estudo de caso em organizações que fazem parte da APF, por meio de questionário eletrônico.

1.4 JUSTIFICATIVA

Foi constatado o baixo número de contribuições em pesquisas relacionadas à melhoria da governança e gestão da TIC na APF. Em um contexto geral, pode-se considerar que a APF está em um estado de desgovernança, ou seja, não são adotados princípios, boas práticas e/ou ferramentas que promovam agregação de valor, alcance dos objetivos e benefícios para a organização. Em TCU (2017) são definidas dimensões, em que o mesmo aborda: Liderança da alta administração, Estratégias e Planos, Informações, Pessoas, Processos e Resultados de TI. Para que a melhoria da maturidade da governança seja alcançada, devemos adotar algum mecanismo que viabilize esse objetivo.

Podemos considerar como solução, a adoção de boas práticas, para que seja possível melhorar a maturidade dos processos, a fim de alcançar e adquirir qualidade em sua gestão. E contribuindo então para superar os desafios relativos à APF, como a racionalização dos gastos públicos, equilíbrio fiscal, estabilidade monetária e investimentos em setores. Estes são direitos previstos pela Constituição da República Federativa do Brasil de 1988, sendo eles: infraestrutura, saúde, educação, mobilidade urbana, habitação e segurança.

1.5 ESTRUTURA DO TRABALHO

Este trabalho está dividido em sete capítulos. No primeiro, é apresentada a Introdução, contendo a contextualização, objetivos gerais e específicos, problemática e justificativa. Já no segundo capítulo, é apresentado o Referencial Teórico e trabalhos relacionados à área de Governança, que servirá de base para o entendimento do tema a ser

apresentado. O terceiro capítulo apresenta a Metodologia adotada na produção do referente trabalho. O quarto capítulo apresenta a Análise das Boas Práticas de GovTIC. O quinto capítulo apresenta os modelos BPM para auxiliar na implementação de GovTIC. No sexto capítulo é apresentado os Resultados da Aplicação do Questionário em organizações da APF. E no sétimo capítulo são apresentadas as Conclusões, além das dificuldades e ameaças a validade, trabalhos futuros e as contribuições relacionadas a este trabalho.

2 REFERENCIAL TEÓRICO

Este capítulo serve como base teórica para obtenção dos principais conceitos inerentes a governança, os quais trarão maior clareza e melhor entendimento sobre o contexto a ser apresentado nas seções a seguir. São abordados os conceitos relevantes a Governança Corporativa; Governança Corporativa Pública; Governança de TIC; e Governança de TIC na APF.

2.1 GOVERNANÇA CORPORATIVA

A Governança Corporativa pode ser definida como o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselhos de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas (IBGC, 2015).

Uma boa Governança Corporativa é um processo, tanto em termos de definição de estruturas, quanto de implementação de melhores práticas (IFC; OCDE, 2009). Esta contribui para um desenvolvimento econômico sustentável, proporcionando melhorias no desempenho das organizações (YOSHITAKE et al., 2014). Empresas que praticam a Governança Corporativa têm maior probabilidade de obter vantagens financeiras em momentos de necessidade (IFC; OCDE, 2009).

Ao discorrer sobre governança, deve-se ter em mente que a mesma é baseada em três pilares básicos, conforme Brasil (2014), sendo eles:

- a) Liderança: conjunto de práticas ou comportamentos que viabilizem o exercício da boa governança;
- b) Estratégia: conjunto de práticas para definição dos objetivos, indicadores e metas, alinhamento estratégico entre unidades e organizações envolvidas; e
- c) Controle: envolve elementos da teoria da agencia², sendo eles a tríade, transparência, prestação de contas e responsabilização (*accountability*).

As organizações de modo geral, possuem visão, missão e valores a serem seguidos. Estes por sua vez agregam valor e servem como referência para definir os objetivos da organização. A Governança Corporativa possui boas práticas, que tem como finalidade auxiliar no alcance dos objetivos e contribuem para a qualidade da gestão da organização.

² Teoria da agencia: descreve a relação entre duas partes envolvidas no contexto institucional – o Principal e o Agente.

Conforme o Instituto Brasileiro de Governança Corporativa (IBGC) (2015), as boas práticas são:

- a) Transparência: disponibilização de informações relevantes às partes interessadas (*stakeholders*);
- b) Equidade: tratamento justo e igualitário para todas as partes interessadas (*stakeholders*);
- c) Prestação de Contas (*accountability*): os indivíduos e órgãos envolvidos na governança da organização, devem prestar contas de sua atuação e assumir a responsabilidade pelos seus atos; e
- d) Responsabilidade Corporativa: os indivíduos e órgãos envolvidos na governança da organização devem zelar pelos insumos e recursos que lhe são disponibilizados, ou seja, utilizá-los de forma eficiente e eficaz, a fim de reduzir os riscos operacionais e financeiros, objetivando a longevidade da organização.

2.2 GOVERNANÇA CORPORATIVA PÚBLICA

A Governança Corporativa Pública pode ser definida como conjunto de princípios e práticas que conduzem a administração pública ao alcance da eficiência, eficácia e efetividade nos seus resultados, por meio de um melhor gerenciamento dos seus processos e de suas atividades, promovendo a prestação de contas responsável (*accountability*) por parte dos gestores e a transparência de suas ações (BIZERRA; ALVES; RIBEIRO, 2012).

Entre os princípios básicos, vale ressaltar que a *accountability* pode ser considerada a de maior destaque e importância, pois a mesma está presente em diversos autores, apesar dos seus distintos enfoques, conforme (BIZERRA; ALVES; RIBEIRO, 2012; LINCZUK, 2012; MATIAS-PEREIRA, 2010). A *accountability* em sua tradução literal significa responsabilidade, ou seja, responsabilidade pelo que, perante quem e quando do gestor profissional em prestar contas e identificar os envolvidos na gestão do setor público.

A Governança Pública pode ser vista como meio de alcançar os objetivos da sociedade. Esta por sua vez, conforme Brasil (2014), envolve três funções básicas que servem como alicerce para uma boa governança, sendo elas: avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e a prestação de serviços de interesse da sociedade. Segundo ABNT (2009c), estas funções podem ser descritas a partir do seguinte contexto:

- a) Avaliar o ambiente, os cenários, o desempenho e os resultados atuais e futuros;

- b) Direcionar e orientar a preparação, a articulação e a coordenação de políticas e planos, alinhando as funções organizacionais às necessidades dos *stakeholders* e assegurando o alcance dos objetivos predeterminados; e
- c) Monitorar os resultados, o desempenho e o cumprimento de políticas e planos, comparando com as metas estabelecidas e expectativas dos *stakeholders*.

2.3 GOVERNANÇA DE TIC

A GovTIC é o termo usado para descrever a forma como as pessoas responsáveis pela governança de uma organização considerarão a TIC em supervisão, monitoramento, controle e direção (ITGI, 2014). Ou seja, formular o controle e direcionar o uso atual e futuro da TIC. Significa avaliar e direcionar o uso da TIC para dar suporte à organização e monitorar seu uso para realizar os planos. Inclui a estratégia e as políticas de uso da TIC dentro da organização (ABNT, 2009c).

Para Weill e Ross (2006), a GovTIC é a definição dos direitos decisórios e do *framework* de responsabilidades que estimulam comportamentos desejáveis na utilização da TIC. O principal objetivo da GovTIC é alinhar o setor de TI aos requisitos do negócio, considerando soluções de apoio, assim como a garantia da continuidade dos serviços e a mitigar a exposição do negócio aos riscos da TIC (FERNANDES; ABREU, 2014).

É importante ressaltar a diferença entre os termos Gestão de TIC e Governança de TIC. Segundo Peterson (2004), existe uma clara diferença entre elas. A Gestão de TIC tem como foco o fornecimento interno de serviços de TI e gerenciamento de suas operações atuais, enquanto a GovTIC abrange áreas mais amplas, como a execução de demandas presentes e futuras, tanto dos negócios (foco interno), quanto dos clientes (foco externo). E conforme *Control Objectives For Information end Related Technology*³ (COBIT) 5 (ISACA, 2012), a Gestão é responsável pelo planejamento, desenvolvimento, execução e monitoramento em conformidade com as diretrizes a fim de atingir os objetivos organizacionais. Já a governança define a direção por meio de priorizações e tomadas de decisão, monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos pela organização.

³ COBIT 5: <http://www.isaca.org/cobit/pages/default.aspx>

2.4 GOVERNANÇA DE TIC NA APF BRASILEIRA

A GovTIC pode ser vista como meio de otimizar o uso dos recursos de TIC no âmbito da APF. Entretanto, para que isso seja possível, se faz necessário que alguns órgãos sejam incumbidos da criação, manutenção e evolução contínua dos processos de regimento e fiscalização destes recursos. A seguir serão apresentados os órgãos responsáveis por tais atividades.

2.4.1 Sistema de Administração de Recursos de Tecnologia da Informação

O Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), foi atualizado pelo Decreto nº 7.579 de 11 de outubro de 2011, com o objetivo de organizar a operação, controle, supervisão e coordenação dos recursos de tecnologia da informação da administração direta, autárquica e fundacional do Poder Executivo Federal (adaptado de BRASIL, 2013). Atualmente, o SISP é composto por 222 órgãos da APF (BRASIL, 2015b).

Os órgãos que compõem o SISP possuem uma grande diversidade. Podemos observar que o mesmo é formado por: agências nacionais, banco central, centros federativos, centros de tecnologias, comando das forças armadas, conselhos, fundações, institutos, ministérios, secretarias, universidades entre outros órgãos.

Conforme Decreto nº 7.579 em Brasil (2011), integram o SISP:

- I - Órgão Central, a Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão;
- II - Órgãos Setoriais, representadas por seus titulares, as unidades de administração dos recursos de tecnologia da informação dos Ministérios e dos órgãos da Presidência da República;
- III - Comissão de Coordenação, formada pelos representantes dos Órgãos Setoriais, presidida por representante do Órgão Central;
- IV - Órgãos Seccionais, representadas por seus titulares, as unidades de administração dos recursos de tecnologia da informação das autarquias e fundações;
- e
- V - Órgãos Correlatos, representados pelos seus titulares, as unidades desconcentradas e formalmente constituídas de administração dos recursos de tecnologia da informação nos Órgãos Setoriais e Seccionais.

Para Brasil (2015a), o SISP

promove a integração e a articulação entre os programas de governo, projetos e atividades na definição de políticas, diretrizes e normas para a gestão dos recursos de TI. Estimula o uso racional dos recursos de tecnologia da informação, o seu desenvolvimento e aprimoramento, a padronização, a integração, a interoperabilidade, a normalização dos serviços de produção e disseminação de informações, de forma desconcentrada e descentralizada.

2.4.2 Secretaria de Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão

A Secretaria de Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão (STI/MPOG) é o órgão central do SISP. É sua responsabilidade propor políticas e também planejar, coordenar, supervisionar e orientar normativamente as atividades de gestão dos recursos de TI, governo digital⁴ e segurança da informação (BRASIL, 2015b).

Conforme Decreto nº 7.579 em Brasil (2011), compete ao Órgão Central do SISP:

- I - orientar e administrar os processos de planejamento estratégico, de coordenação geral e de normalização relativos aos recursos de tecnologia da informação abrangidos pelo SISP;
- II - definir, elaborar, divulgar e implementar, com apoio da Comissão de Coordenação, as políticas, diretrizes e normas gerais relativas à gestão dos recursos do SISP e ao processo de compras do Governo na área de tecnologia da informação;
- III - promover a elaboração de planos de formação, desenvolvimento e treinamento do pessoal envolvido na área de abrangência do SISP;
- IV - incentivar ações prospectivas, visando acompanhar as inovações técnicas da área de tecnologia da informação, de forma a atender às necessidades de modernização dos serviços dos órgãos e entidades abrangidos pelo SISP; e
- V - promover a disseminação das políticas, diretrizes, normas e informações disponíveis, de interesse comum, entre os órgãos e entidades abrangidos pelo SISP.

Entre as atividades da STI/MPOG, podem ser citadas também a padronização e transformação digital dos serviços públicos, acessibilidade digital, abertura de dados, incentivo ao uso de *software* público, manutenção e ampliação da Infovia e a divulgação da Política de Governança Digital a partir da Estratégia de Governança Digital (EGD) (BRASIL, 2015b). Esta última será discutida na próxima sessão.

2.4.3 Estratégia de Governança Digital

A EGD pode ser entendida como uma nova forma de gestão para os órgãos públicos e organizações envolvidas com a APF. A estratégia tem como propósito explorar, potencializar e orquestrar sinergias visando uma maior eficácia, eficiência, efetividade e uso racional dos recursos públicos (adaptado de BRASIL, 2016d). A EGD tem como pretensão a promoção de um movimento de simplificação e agilização na prestação dos serviços públicos e de melhoria do ambiente de negócios e da eficiência da gestão pública (adaptado de BRASIL, 2016d).

⁴ Governo Digital refere-se ao uso de tecnologias digitais, como parte integrada das estratégias de modernização governamentais, para gerar benefícios para sociedade.

A EGD foi aprovada pela Portaria nº 68, em Brasil (2016a), no qual compete ao STI/MPOG coordenar a formulação, o monitoramento, a avaliação e a revisão com participação das demais unidades que atuam como órgão central dos sistemas estruturantes do Poder Executivo Federal.

Conforme decreto nº 8.638, Brasil (2016b) define ainda que a EGD deve:

- I - gerar benefícios para a sociedade mediante o uso da informação e dos recursos de tecnologia da informação e comunicação na prestação de serviços públicos;
- II - estimular a participação da sociedade na formulação, na implementação, no monitoramento e na avaliação das políticas públicas e dos serviços públicos disponibilizados em meio digital; e
- III - assegurar a obtenção de informações pela sociedade, observadas as restrições legalmente previstas.

Além da prestação de serviços de forma digital, são pilares da estratégia o estímulo a participação da sociedade nas políticas públicas e a ampliação do acesso à informação (BRASIL, 2016c). A estratégia serve de complemento a política de governança digital e visa convergir e integrar iniciativas de governo digital e de governança digital para ampliar os benefícios e o acesso a direitos e deveres de cidadãos e organizações, de forma mais efetiva, estimular a colaboração em rede e a construção conjunta de iniciativas entre Estado e sociedade (HECKERT; AGUIAR, 2016).

2.5 AVALIAÇÃO DA GOVERNANÇA DE TIC NA APF DO BRASIL

A avaliação da GovTIC na APF do Brasil é realizada periodicamente pelo TCU a cada dois anos, possibilitando vislumbrar a situação da GovTIC na APF. Os últimos levantamentos efetuados ocorreram em 2010, 2012, 2014 e 2016, sendo estes detalhados respectivamente pelos Acórdãos 2.308/2010, 2.585/2012, 3.117/2014, 8.127/2016-6 todos do Plenário.

Os dados são obtidos a partir de questionário realizado pelo TCU, e servem como base para elaboração dos Acórdãos. Segundo o TCU (2017), este questionário é baseado em:

- a) Boas práticas reconhecidas pela comunidade internacionalmente;
- b) Legislação vigente; e
- c) Jurisprudência do TCU.

Ainda em TCU (2017), para avaliação das organizações especificamente, estas são distribuídas em seis grupos conforme características próprias, sendo eles:

- a) EXE-Sest: empresas públicas federais e as sociedades de economia mista;
- b) EXE-Sisp: organizações que fazem parte do Sisp;

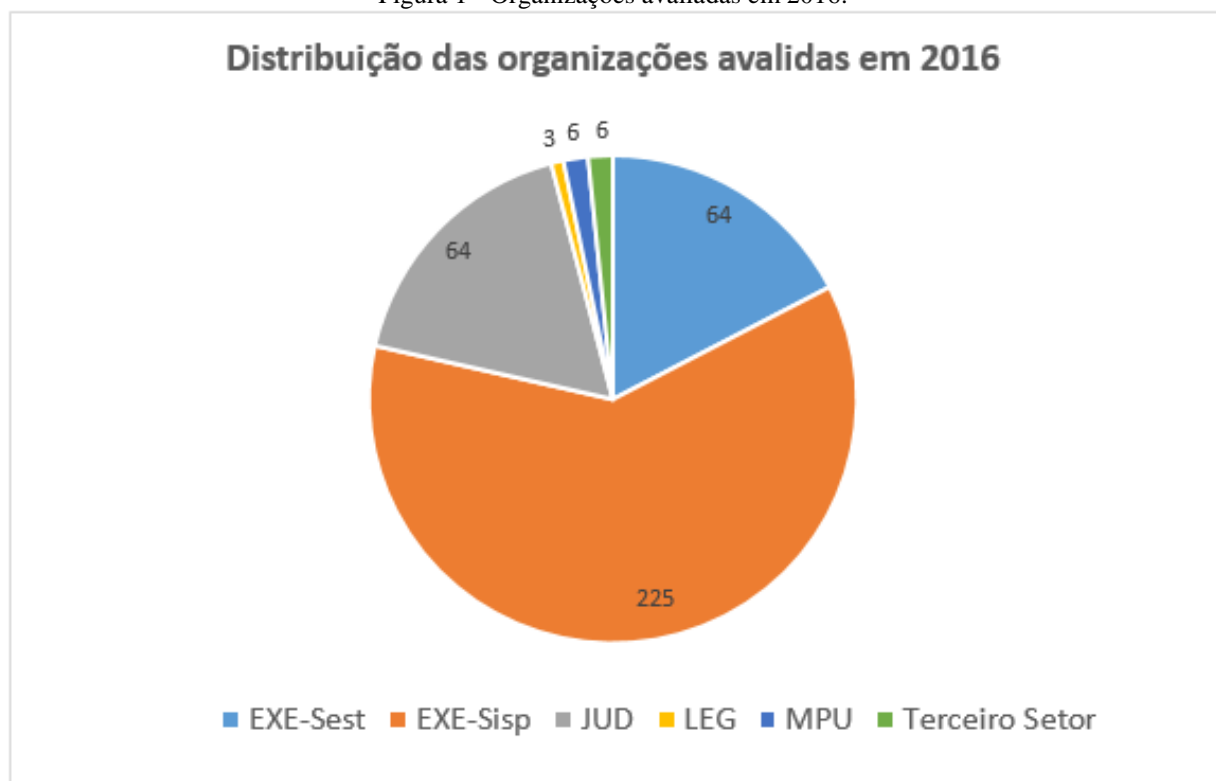
- c) JUD: organizações que fazem parte do Poder Judiciário;
- d) LEG: organizações que fazem parte do Poder Legislativo;
- e) MPU: organizações que fazem parte do Ministério Público da União (MPU); e
- f) Terceiro Setor: organizações que não fazem parte de nenhum dos grupos acima citados.

Estas organizações, após aplicação de questionário são agrupadas por nível de capacidade em GovTIC. São eles: inicial, básico, intermediário e aprimorado (TCU, 2017).

2.5.1 Situação Atual da Governança de TIC no Governo Federal, na Visão do TCU

Conforme levantamento feito pelo TCU em 2016, foram enviados 379 ofícios, porém apenas 368 organizações participaram efetivamente do questionário. Os resultados podem ser observados na Figura 1.

Figura 1 - Organizações avaliadas em 2016.



Fonte: TCU (2017).

Conforme é observado na Figura 1, a maior porcentagem dos órgãos faz parte do SISP, aproximadamente 61%. Tal dado deixa claro o quão grande e importante é o SISP devido ao enorme grupo de órgãos que o compõem. Isso implica na influência direta no iGovTI.

Para que seja possível realizar melhor a avaliação, o TCU divide a GovTIC em dimensões, no qual cada uma possui boas práticas a serem seguidas. Cada prática possui um número de questões relacionadas, que servem de base para definição do iGovTI. Podemos observar no Quadro 1 as práticas, sua definição e os temas específicos abordados por cada dimensão.

Quadro 1 - Dimensões da TIC.

Dimensão	Definição	Temas Específicos
Liderança da Alta Administração	Refere-se aos elementos essenciais de governança corporativa e de TIC.	<ul style="list-style-type: none"> • Sistema de governança corporativa; • Sistema de governança de TIC; • Resultados de TIC; • Risco de TIC; • Pessoal de TIC; • Transparência da gestão e uso da TIC; • Monitoramento da governança e gestão de TIC; e • Capacidade da Auditoria Interna.
Estratégias e Planos	Avalia os controles da gestão de estratégias e planos corporativos e de TIC.	<ul style="list-style-type: none"> • Planejamento estratégico institucional; e • Planejamento de TIC.
Informações	Avalia os controles da gestão da informação, contemplando inclusive a prática de transparência.	<ul style="list-style-type: none"> • Informatização dos processos organizacionais; e • Transparência das informações relacionadas à gestão e uso da TI.
Pessoas	Avalia os controles da gestão de pessoas em TI.	<ul style="list-style-type: none"> • Desenvolvimento de competências de TI; • Desempenho do pessoal de TI; e • Força de trabalho de TI.
Processos	Refere-se aos controles da gestão de processos em TI.	<ul style="list-style-type: none"> • Processos de gerenciamento de serviços de TI; • Gerenciamento de nível de serviço de TI; • Gestão de risco de TI; • Gestão corporativa da segurança da informação; • Processo de <i>software</i>; • Gerenciamento de projetos de TI; • Contratações de serviços de TI; • Processo de planejamento das contratações de TI; • Processo de gestão dos contratos de TI; e • Perfil das contratações de TI.
Resultados da TI	Refere-se ao desempenho da organização na gestão e uso da TI.	<ul style="list-style-type: none"> • Capacidade da organização de definir e alcançar os objetivos de TI; • Gerir projetos de TI; • Serviços que sustentam os processos organizacionais; e • Serviços disponíveis ao cidadão/cliente.

Fonte: Adaptado de Fernandes e Abreu (2014); TCU (2017).

O iGovTI foi criado em 2010, com o propósito de orientar as organizações públicas no esforço de melhoria da governança e da gestão de TC. O índice também permite ao TCU

avaliar a efetividade das ações adotadas para induzir a melhoria da situação de GovTIC na APF (adaptado de TCU, 2017).

O iGovTI é o resultado da consolidação do questionário de governança de TIC por meio das formulas observadas no Quadro 2, que resulta em um valor que varia de 0 a 1. A fórmula do iGovTI2016 manteve-se igual a fórmula definida para o iGovTI2014 (TCU, 2017).

Quadro 2 - Cálculo do iGovTI.

Fórmula	Representação Matemática	Composta	Definição
Questões	$q_n = a_1 i_1 + a_2 i_2 + \dots + a_n i_n$	a_n	Valores atribuídos a cada categoria de resposta
		i_n	Peso no item na questão
Dimensões	$d_n = b_1 q_1 + b_2 q_2 + \dots + b_n q_n$	b_n	Nota de uma questão respondida
		q_n	Peso dessa questão
iGovTI 2014	$iGovTI_{2014} = d_1 p_1 + d_2 p_2 + \dots + d_n p_n$	d_n	Nota da dimensão
		p_n	Peso da dimensão

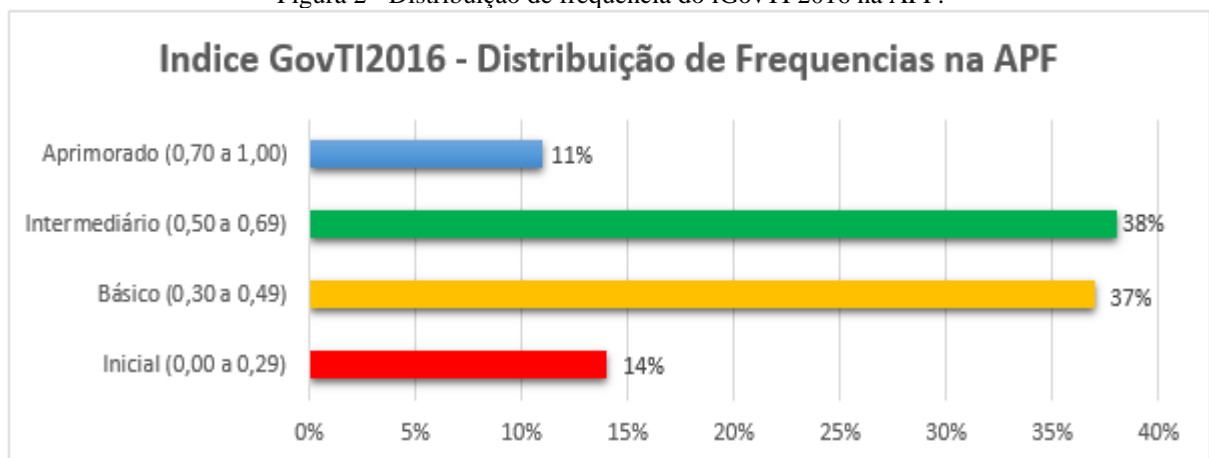
Fonte: Adaptado de TCU (2014).

As organizações podem ser agrupadas por nível de capacidade. Estes níveis indicam qual a situação atual que as organizações se encontram, são eles:

- a) Inicial com $iGovTI < 0,3$;
- b) Básico com $0,3 \geq iGovTI < 0,5$;
- c) Intermediário com $0,5 \geq iGovTI < 0,7$; e
- d) Aprimorado com $0,7 \geq iGovTI$.

A Figura 2 apresenta a situação do iGovTI por segmento da APF em 2016.

Figura 2 - Distribuição de frequência do iGovTI 2016 na APF.



Fonte: TCU (2017).

Conforme observado na Figura 2, podemos destacar que no nível inicial estão 14% das organizações avaliadas. Em contrapartida, somente 11% das organizações tem seu nível de governança aprimorado. A maior parte das organizações, 51%, encontram-se nos níveis básico e inicial, isso quer dizer que, elas possuem baixas condições de governar a TIC de forma a produzir valor para a organização (TCU, 2017).

2.6 BOAS PRÁTICAS PARA MELHORIA DA GOVTIC

O aprimoramento da GovTIC é uma das necessidades da APF. Conforme apresentado em (TCU, 2017), existem como soluções para esse propósito diversas metodologias e *frameworks*, os quais podem auxiliar a governabilidade dos recursos nas organizações da APF.

Para elaboração deste trabalho identificamos diversas boas práticas de GovTIC, conforme Quadro 3.

Quadro 3 - Boas práticas de GovTIC identificadas.

Autor(es)	Boas práticas
Fernandes e Abreu (2014)	<ul style="list-style-type: none"> • Norma Brasileira (NBR) <i>International Organization for Standardization/International Electrotechnical Commission</i> (ISO)/(IEC) 20000, 27001, 27002 e 38500; • NBR ISO 31000; • <i>Capability Maturity Model - Integration</i> (CMMI); • Modelo de Melhoria de Processo de <i>Software</i> Brasileiro (MPS.BR); e • <i>Information Technology Infrastructure Library</i> (ITIL).
Loureiro; Penha e Nascimento (2012)	<ul style="list-style-type: none"> • COBIT 5; e • ITIL
Silva et al. (2017a)	<ul style="list-style-type: none"> • CMMI • COBIT 5 • <i>Committee of Sponsoring Organizations</i> (COSO); e • ITIL
Silva et al. (2017b)	<ul style="list-style-type: none"> • COBIT 5; • ITIL; • NBR ISO/IEC 20000-1 e 27001; e • <i>Project Management Body of Knowledge</i> (PMBOK)
TCU (2016)	<ul style="list-style-type: none"> • CMMI; • COBIT 5; • Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação; • ITIL; • MPS.BR; • NBR ISO/IEC 12207, 15504, 20000-2, 27002, 27005, 38500; e • PMBOK.
TCU (2017)	<ul style="list-style-type: none"> • NBR ISO/IEC 20000-2, 27002 e 38500; • ITIL; e • COBIT.

Fonte: Os Autores, 2017.

Para elaboração deste trabalho utilizaremos as boas práticas:

- a) CMMI;
- b) COBIT 5;
- c) Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação;
- d) ITIL;
- e) NBR ISO 31000;
- f) NBR ISO/IEC 12207, 20000-2, 27001, 27002, 27005 e 38500; e
- g) PMBOK.

O *framework* CMMI tem como objetivo a melhoria de processos da organização. Foi lançado em 2002 pelo *Software Engineering Institute* (SEI) dos Estados Unidos, e tem sua origem advinda do *Capability Maturity Model* (CMM).

Segundo Rouiller et al. (2006), o CMMI integra diversos modelos de maturidade publicados pela SEI e incorporar lições assimiladas na utilização ao longo dos anos. O CMMI trabalha voltado sobre dois conceitos fundamentais, sendo eles o de maturidade e capacidade. Quanto a estrutura do CMMI, segundo (SOMMERVILLE, 2011; ROUILLER et al., 2006), é dividido em:

- a) Níveis de maturidade: inicial, gerenciado, definido, gerenciado quantitativamente e otimizado; e
- b) Áreas de processo: gerenciamento de processos, gerenciamento de projetos, engenharia e suporte.

O COBIT foi desenvolvido pela *Information Systems Audit and Control Association* (ISACA) (2012). Ele fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI, ou seja, ajuda a agregar valor por meio da TI, mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos.

Ainda segundo ISACA (2012), o COBIT divide-se em cinco princípios básicos, os quais são:

- a) Atender às necessidades das partes interessadas (*Stakeholders*), traduzindo os objetivos corporativos de alto nível em objetivos de TI específicos e gerenciáveis, mapeando-os em práticas e processos específicos;
- b) Cobrir a organização de ponta a ponta, integrando os interesses e objetivos, de tudo e todos, interna e externamente;
- c) Aplicar um *framework* único e integrado, se alinhando a outros padrões e modelos importantes em um alto nível, como normas e boas práticas relacionadas a TI;

- d) Permitir uma abordagem holística, definindo um conjunto de habilitadores para suportar a implementação de um sistema abrangente de gestão e GovTIC, sendo eles: princípios, políticas e modelos; processos, estruturas organizacionais, cultura, ética e comportamento; informação; serviços, infraestrutura e aplicativos; e pessoas, habilidades e competências; e
- e) Distinguir a governança da gestão, compreendendo suas diferentes atividades, modelos organizacionais e propósitos.

O COBIT 5 define um conjunto de habilitadores para as camadas de governança e gerenciamento de TI. Este trabalho será limitado apenas a camada de gerenciamento, que é definida por quatro domínios, no qual iremos abordar apenas os domínios *Align, Plan and Organize* (APO) e *Build, Acquire and Implement* (BAI) (CHIARI, 2016).

O COSO, conforme COSO (2013), tem como propósito fornecer liderança de pensamento no desenvolvimento de estruturas abrangentes e diretrizes sobre controles internos, gerenciamento de riscos corporativos e fraude para aprimorar a performance e supervisão organizacional e reduzir a extensão das fraudes nas organizações.

O Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação em (TCU, 2012), contém recomendações referentes ao planejamento das contratações de soluções de TI, sob o ponto de vista do controle externo da APF, baseadas na legislação, na jurisprudência e nas melhores práticas do mercado, incluindo sugestões de controles internos para tratar riscos relativos ao processo de contratação de soluções de TI.

ITIL é um conjunto de livros com boas práticas para o gerenciamento de serviços de TI, desenvolvida pelo *Office of Government Commerce* (OGC) do Reino Unido. Conforme análise de Ferreira e Jones (2014), ela se estrutura no conjunto de boas práticas já consolidadas pelas grandes organizações focadas em TI, além de estar alinhada com a ISO 20.000, norma esta que orienta a indústria de TI no gerenciamento e aperfeiçoamento de seus serviços. Conforme Magalhães e Pinheiro (2007), a ITIL é um conjunto de melhores práticas que vem ao encontro do novo estilo de vida imposto as áreas de TI, que habilita o incremento da maturidade do processo de gerenciamento de TI.

A atual versão da ITIL é a V3, lançada em 2007 e tem o foco na eficiência e eficácia dos serviços em produção. A ITIL V3 é composta de seis publicações, sendo cinco livros e um livro resumo, sendo eles:

- a) Estratégia do serviço (*Service Strategy*);
- b) Projeto de serviço ou Desenho de serviço (*Service Design*);
- c) Transição do serviço (*Service Transition*);
- d) Operação do serviço (*Service Operation*);

- e) Melhoria continua do serviço (*Continual Service Improvement*); e
- f) Introdução ao ciclo de vida do serviço (*The Service Lifecycle Introduction*).

O MPS.BR, conforme Softex (2017), é um programa com apoio do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), que teve início em 2003 e tem como objetivo melhorar a capacidade de desenvolvimento de *software*, serviços e as práticas de gestão de recursos humanos na indústria de TIC. Já Koscianski e Soares (2007) complementa que ele visa atender à necessidade de implantar os princípios de engenharia de *software* de forma adequada ao contexto das empresas brasileiras, seguindo as principais abordagens internacionais para definição, avaliação e melhoria de processos de *software*.

A NBR ISO/IEC 20000-2 fornece orientações sobre a aplicação de um Sistema de Gerenciamento de Serviços, com base na NBR ISO/IEC 20000-1. Esta parte da norma fornece exemplos e sugestões para permitir que as organizações interpretem e apliquem a NBR ISO/IEC 20000-1 (ABNT, 2013a).

A NBR ISO/IEC 12207 formaliza os Processos do Ciclo de Vida do *Software* por meio de um *framework* com terminologias de processos bem definidos, ao invés de forçar a utilização de um determinado modelo de ciclo de vida ou método de desenvolvimento de *software* (ABNT, 2009b).

A Norma ISO/IEC 15504 foi elaborada a partir do projeto *Software Process Improvement and Capability dEtermination* (SPICE) (KOSCIANSKI; SOARES, 2007). A Norma presta-se à realização de avaliações de processos de *software* com dois objetivos: a melhoria de processos e a determinação da capacidade de processos de uma unidade organizacional (ABNT, 2008).

Conforme Fernandes e Abreu (2014) a ISO/IEC possui a série de normas 27000 sobre segurança de informação. Por meio do uso da série 27000, as organizações podem desenvolver e implementar uma estrutura para gerenciar a segurança de seus ativos de informação, incluindo informações financeiras, propriedade intelectual e detalhes do empregado, ou informações confiadas a eles por clientes ou terceiros (ISO, 2014).

A NBR ISO/IEC 27001 especifica os requisitos necessários para um Sistema de Gerenciamento de Segurança da Informação (SGSI) e a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes (ABNT, 2006).

Já a NBR ISO/IEC 27002 estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Esta Norma pode servir como um guia prático para desenvolver os procedimentos de

segurança da informação da organização e as eficientes práticas de gestão da segurança (ABNT, 2013b).

Por último a NBR ISO/IEC 27005 fornece diretrizes para o processo de gestão de riscos de segurança da informação de uma organização, atendendo particularmente aos requisitos de um SGSI (ABNT, 2011).

A NBR ISO 31000 fornece princípios e diretrizes genéricas para a gestão de riscos, sendo utilizada para harmonizar os processos de gestão de riscos. Para isso, ela orienta que deve-se levar em consideração as necessidades variadas de uma organização específica, como seus objetivos, contexto, estrutura, operações, processos e entre outras (ABNT, 2009a). Ela fornece técnicas de avaliação de riscos que podem ser adaptadas às condições e necessidades da organização, por meio do fornecimento de um quadro mais geral que pode acomodar todos os tipos de gerenciamento de riscos em um *framework* ISO 31000 (ERNAWATI; SUHARDIB; NUGROHO, 2012).

A NBR ISO/IEC 38500 é relacionada a governança corporativa de TI e tem como objetivo fornecer uma estrutura de princípios para os dirigentes (incluindo proprietários, membros do conselho de administração, diretores, parceiros, executivos ou similares) utilizarem na avaliação, gerenciamento e monitoramento do uso da TI em suas organizações (FERNANDES; ABREU, 2014). Ainda conforme a Associação Brasileira de Normas Técnicas (ABNT) (2009c), a norma oferece uma estrutura eficaz para governança de TI que ajuda alta administração das organizações a entender e cumprir suas obrigações legais, regulamentares e éticas com relação ao uso da TI.

Por último, o Guia PMBOK fornece diretrizes para o gerenciamento de projetos individuais e define os conceitos relacionados com o gerenciamento de projetos. Ele também descreve o ciclo de vida de gerenciamento de projetos e seus respectivos processos, assim como o ciclo de vida do projeto (PMI, 2013).

2.7 TRABALHOS RELACIONADOS

Os trabalhos na área de GovTIC na APF tem contribuído de maneira efetiva para geração de valor e aprimoramento da prática da governança nas organizações, auxiliando a melhoria da teoria e prática dos processos de GovTIC. Entretanto, poucos são os trabalhos voltados para as Boas Práticas de Governança de TIC com intuito de nortear as organizações da APF a melhorar seu iGovTI, conforme requisitado pelo TCU.

Para seleção dos trabalhos relacionados foi utilizado o trabalho de Silva et al. (2017a) por este apresentar o estado da arte voltado para GovTIC. A seguir serão apresentados trabalhos relevantes ao tema:

Silva et al. (2017a), apresentam uma quasi revisão sistemática para identificar, caracterizar e resumir as principais evidências sobre a Governança Pública de TIC, a fim de analisar os métodos, técnicas, modelos, *framework*, guias e/ou boas práticas de Governança Pública de aplicação em um ambiente de TI, ajudando os gestores de TIC por meio de um estudo secundário. Podemos citar como limitação desta quasi revisão sistemática, a não existência de um estudo de caso para verificação e validação da mesma.

Silva et al. (2017b), apresentam um mapeamento sistemático afim de identificar e sistematizar em quais países existe iniciativas para governança de TIC na APF. Este artigo ainda, relata quais métodos e/ou técnicas são utilizados na APF e destaca quais Universidades e Autores têm contribuído neste campo. Podemos citar como limitação deste mapeamento sistemático, a não realização de um estudo de caso para verificar e validar se realmente são adotados os métodos e/ou técnicas na APF identificadas.

Oliveira Júnior (2015), apresenta uma proposta de um plano baseado nas exigências legais pertinentes a APF, no qual, é detalhado um conjunto de ações necessárias para que estejam em conformidade com o que a legislação exige às instituições Federais de Ensino. O ciclo do plano é baseado no *framework* Modelo Ágil no apoio à Governança em TIC (MANGve) e tem finalidade de possibilitar a melhoria do índice de maturidade dos processos de GovTIC. Podemos citar como limitação deste trabalho, a não realização de um estudo de caso com o plano apresentado e que o ciclo dele não direciona a organização para melhoria da dimensão que possui déficit.

Hamid e Sulaiman (2016), adotam uma ferramenta de avaliação do processo de Maturidade COBIT 4.1, desenvolvido pela ISACA, para assegurar a maturidade do processo dos atuais Departamentos de Serviço Público da Malásia. Ela é uma ferramenta de diagnóstico baseada no modelo de maturidade COBIT, o qual inclui a implementação e melhoria continua do kit de ferramenta de GovTIC. Esta ferramenta auxilia na implementação da governança de TIC na organização alvo. A limitação do trabalho de Hamid e Sulaiman é que a forma de obter a GovTIC não está direcionada com as dimensões do TCU, a mesma faz referência ao governo da Malásia.

Vasconcellos (2013), em seu trabalho propõe e testa um modelo de mensuração do uso da metodologia de BPM sob o ponto de vista de profissionais da área de TI, com foco na GovTIC. Ele descreve as práticas de BPM e de GovTIC, a teoria a respeito de alinhamento de

práticas de BPM e GovTIC, verifica a percepção dos respondentes da pesquisa aos conceitos e aplicação nas organizações de BPM e de GovTIC e analisa os indicadores de alinhamento de BPM com a GovTIC com a percepção dos respondentes. Como limitação deste trabalho, apesar da verificação de boas práticas, não foram seguidas as recomendações do TCU, órgão regulador vigente para GovTIC.

No Quadro 4, é ilustrado o comparativo de características dos trabalhos relacionados.

Quadro 4 - Comparativo de características dos trabalhos relacionados.

Trabalhos	Conformidade com TCU (dimensões)	Comparação das Boas Práticas (COBIT, ITIL, entre outras)	Direcionamento para a dimensão de Processos	Estudo de Caso
Silva et al. (2017a)	Sim	Sim	Não	Não
Silva et al. (2017b)	Não	Sim	Não	Não
Oliveira Júnior (2015)	Sim	Sim	Não	Não
Hamid e Sulaiman (2016)	Não	Não	Não	Sim
Vasconcellos (2013)	Não	Sim	Não	Sim

Fonte: Os Autores, 2017.

Conforme o Quadro 4, o mesmo segue a seguinte configuração: nas colunas estão dispostos os pontos de observações no trabalho e nas linhas indica o que ele possui ou não. Já a coluna "Direcionamento para a dimensão de Processos", é possível notar que nenhum dos trabalhos relacionados fazem menção a essa temática, o que resulta em um dos direcionamentos do presente trabalho.

3 METODOLOGIA

Neste capítulo tem-se a descrição da metodologia adotada para este trabalho de pesquisa. Na seção 3.1, apresenta-se a classificação da pesquisa quanto a sua natureza, abordagem do problema, objetivo e procedimentos técnicos adotados no seu desenvolvimento. Em seguida, na seção 3.2, têm-se a instrumentação para a criação do modelo processo para a implantação das boas práticas observadas na dimensão de Processos, conforme definido pelo TCU e o questionário de verificação e validação.

3.1 CLASSIFICAÇÃO DA PESQUISA

O objetivo geral desta pesquisa foi atingido, pois realizou uma análise de qual(is) boa(s) prática(s) adotar em organizações da APF para melhorar o índice de maturidade iGovTI na dimensão de Processos, conforme definido pelo TCU, visando o gerenciamento de projetos de TI para o desenvolvimento e implantação de soluções em TI. O TCU (2017) afirma que, merece atenção o elevado percentual de organizações que não executam processos de gerenciamento de projeto de TI, situação que eleva o risco de insucesso de seus projetos, principalmente pela complexidade que, em geral, envolve o desenvolvimento e implantação de soluções de TI.

Quanto à natureza, esta pesquisa classifica-se como aplicada, visto que objetiva gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos (SILVEIRA; CÓRDOVA, 2009), ou seja, destina-se a direcionar as organizações da APF a minimizar o déficit de GovTIC na dimensão de Processos. Com isso, a minimização se dará por meio da modelagem e aplicação de processos (BPM) das boas práticas a serem adotadas.

Quanto a abordagem dos dados, esta pesquisa classifica-se como qualitativa. Malhotra (2001) define como uma técnica de “...pesquisa não-estruturada, exploratória, baseada em pequenas amostras, que proporciona *insights* e compreensão do contexto do problema” que está sendo estudado, ou seja, é necessário identificar a(s) boa(s) prática(s) de GovTIC na dimensão de Processos, a qual(is) será(ão) utilizada(s) para a criação do modelo de processos.

Quanto aos objetivos, esta pesquisa classifica-se como descritiva. Fontelles et al. (2009) define que é aquela que visa apenas a observar, registrar e descrever as características de um determinado fenômeno ocorrido em uma amostra ou população, na qual faz o estudo

das boas práticas de GovTIC existentes e um direcionamento dessas para a dimensão de Processos.

Quanto aos procedimentos técnicos utilizados para desenvolver a pesquisa, este trabalho pode ser caracterizado como pesquisa bibliográfica. Fontelles et al. (2009) descreve que é a análise de material já publicado. É utilizada para compor a fundamentação teórica a partir da avaliação atenta e sistemática de livros, periódicos, documentos, textos, mapas, fotos, manuscritos e, até mesmo, de material disponibilizado na internet e etc., pois é por meio da pesquisa bibliográfica das boas práticas que a modelagem de processos será desenvolvida.

Ainda quanto aos procedimentos técnicos, ele também é caracterizado como estudo de caso, conforme Gil (2002), no qual consiste no estudo profundo e exaustivo de um ou poucos objetos, de maneira que permita seu amplo e detalhado conhecimento. Foi realizado estudo de caso em uma organização da APF, com o objetivo da validação e verificação do modelo de boa(s) prática(s) na dimensão de Processos, conforme definido pelo TCU.

3.2 INSTRUMENTAÇÃO

Nesta seção são apresentadas as instrumentações que foram utilizadas para desenvolver este trabalho.

3.2.1 Instrumentação: *Business Process Management*

Existem várias ferramentas para modelagem de processos, mas selecionamos o BPM por estarmos mais familiarizados com sua metodologia.

O BPM é um conjunto de métodos e técnicas que auxiliam a organização na gestão de seu negócio por meio do conhecimento e entendimento de seus processos (ARAÚJO et al., 2004). Outro conceito apresentado por Vasconcellos (2012), indica que o BPM é um conjunto de melhores práticas aplicadas ao gerenciamento e controle dos processos de negócio com o uso da tecnologia para otimizar os resultados da organização. Já para Fernandes e Abreu (2014), o BPM apresenta-se como modelo complementar às práticas de Governança de TI porque possibilita uma visão clara e controlada dos processos da governança, capacitando a organização na visão do valor da TI.

Dentre as diversas ferramentas existentes que auxiliam no desenvolvimento de modelos com a notação BPM, podemos citar: Bizagi⁵, Microsoft Visio⁶, Microsoft Enterprise Architecture⁷ e Oracle BPM⁸. Para elaboração deste modelo, utilizamos a ferramenta Bizagi, por esta possuir versão gratuita e ser reconhecida como uma das mais difundidas e completas. Nesta versão é disponível apenas a funcionalidade de modelagem de processos, porém em sua versão completa, na qual é necessário efetuar a compra da licença, está disponível além da modelagem, a possibilidade de gerar uma aplicação ou *workflow* dinâmico do modelo com o Bizagi Studio e o controle de processos automatizados com o Bizagi Engine.

3.2.2 Instrumentação: Questionário de Verificação e Validação

O questionário de validação realizado está descrito no Apêndice B, que detalha claramente as perguntas separadas em duas seções, sendo elas:

- a) Modelos BPM; e
- b) Análise das Boas Práticas.

A divisão por seções auxilia o respondente a focar nos diferentes aspectos aos quais as questões abordam e tem o intuito de proporcionar um melhor entendimento delas.

Para a elaboração do questionário foi utilizada a escala Likert, segundo Oliveira Júnior (2015), ela é considerada a mais utilizada em pesquisas de opinião. No qual segue o seguinte padrão:

- a) Discordo Totalmente;
- b) Discordo Parcialmente;
- c) Nem Concordo, Nem Discordo;
- d) Concordo Parcialmente; e
- e) Concordo Plenamente.

O questionário foi respondido por gestores ou servidores ligados a GovTIC na APF. A aplicação desse questionário foi por meio de um formulário *web* e cada participante respondeu um total de dezessete perguntas. A participação de cada respondente se dará por meio de convite enviado via e-mail constando as instruções de como preencher o questionário, conforme está descrito no Apêndice A.

⁵ Bizagi: <http://www.bizagi.com/pt>

⁶ Microsoft Visio: <https://products.office.com/pt-br/visio/flowchart-software>

⁷ Microsoft Enterprise Architecture: <https://msdn.microsoft.com/en-us/library/aa286495.aspx>

⁸ Oracle BPM: <http://www.oracle.com/us/technologies/bpm/overview/index.html>

4 ANÁLISE DAS BOAS PRÁTICAS

Neste capítulo é detalhada a análise das boas práticas para cada tema específico da dimensão de Processos, conforme definido pelo TCU. Além de apresentar qual(is) direcionamento(s) as boas práticas indicam para cada tema.

4.1 GERENCIAMENTO DE SERVIÇOS DE TI

Nesta seção a boa prática identificada foi a ITIL. Esta mesma trata quatorze itens, conforme demonstrado o relacionamento entre eles e as práticas no Quadro 5.

Quadro 5 - Boas práticas para Gerenciamento de Serviços de TI.

Item	ITIL
a) a organização executa processo de gerenciamento do catálogo de serviços.	Service Design Capítulo: 4.1 Gerenciamento de Catálogo de Serviços
b) o processo de gerenciamento do catálogo de serviços está formalmente instituído, como norma de cumprimento obrigatório.	Service Design Capítulo: 4.1 Gerenciamento de Catálogo de Serviços
c) a organização executa processo de gerenciamento da continuidade dos serviços de TI.	Service Design Capítulo: 4.5 Gerenciamento de Continuidade de Serviços De TI
d) o processo de gerenciamento de continuidade dos serviços de TI está formalmente instituído, como norma de cumprimento obrigatório.	Service Design Capítulo: 4.5 Gerenciamento de Continuidade de Serviços de TI
e) a organização executa processo de gerenciamento de mudanças.	Service Transition Capítulo: 4.2 Gerenciamento de Mudanças
f) o processo de gerenciamento de mudanças está formalmente instituído, como norma de cumprimento obrigatório.	Service Transition Capítulo: 4.2 Gerenciamento de Mudanças
g) a organização executa processo de gerenciamento de configuração e ativos.	Service Transition Capítulo: 4.3 Gerenciamento de Configuração e Ativos de Serviço
h) o processo de gerenciamento de configuração e ativos está formalmente instituído, como norma de cumprimento obrigatório.	Service Transition Capítulo: 4.3 Gerenciamento de Configuração e Ativos de Serviço
i) a organização executa processo de gerenciamento de liberação e implantação.	Service Transition Capítulo: 4.4 Gerenciamento de Liberação e Implantação
j) o processo de gerenciamento de liberação e implantação está formalmente instituído, como norma de cumprimento obrigatório.	Service Transition Capítulo: 4.4 Gerenciamento de Liberação e Implantação
k) a organização executa processo de gerenciamento de incidentes.	Service Operation Capítulo: 4.2 Gerenciamento de Incidente
l) o processo de gerenciamento de incidentes está formalmente instituído, como norma de cumprimento obrigatório.	Service Operation Capítulo: 4.2 Gerenciamento de Incidentes
m) a organização executa processo de gerenciamento de problemas.	Service Operation Capítulo: 4.4 Gerenciamento de Problemas
n) o processo de gerenciamento de problemas está formalmente instituído, como norma de cumprimento obrigatório.	Service Operation Capítulo: 4.4 Gerenciamento de Problemas

Fonte: Os Autores, 2017.

Para os itens a) e b) do Quadro 5, a ITIL orienta que a criação e o gerenciamento de um Catálogo de Serviços com o objetivo de reunir em um único local as informações sobre todos os serviços já executados pela organização e os previstos para o futuro. Este catálogo deve estar disponível somente para os colaboradores autorizados. Ele demonstra que a estrutura do catálogo de serviços possui dois aspectos, sendo eles: de negócio e tecnológicos. O de negócio é a parte que o cliente visualiza e interage, já o tecnológico é o que dá suporte ao serviço do negócio.

Para os itens c) e d) do Quadro 5, a ITIL orienta que a organização realize o Gerenciamento de Continuidade de Serviço de TI, de modo a assegurar que os serviços continuem sendo oferecidos mesmo após a ocorrência de um desastre. Em caso de interrupções, a organização deve possuir um plano de continuidade dos serviços de TI que determina os prazos máximos para que os serviços sejam restabelecidos. Ela também orienta que seja responsabilidade do gerente conscientizar os colaboradores sobre a importância de realizar o Gerenciamento de Continuidade de Serviço de TI.

Para os itens e) e f) do Quadro 5, a ITIL orienta que a organização execute um processo de Gerenciamento de Mudança, de modo a minimizar incidentes causado pela mudança, reduzindo os riscos e impactos na organização e garantindo que sejam adotados procedimentos padronizados para sua execução eficiente. Com a adoção desse processo todas as mudanças deveram ser registradas, avaliadas, autorizadas, priorizadas, planejadas, testadas, implementadas, documentadas e revisadas de maneira controlada. Ela orienta ainda que esse processo seja aplicado aos departamentos de TI com uma maturidade no Gerenciamento de Serviços de TI.

Para os itens g) e h) do Quadro 5, a ITIL orienta que a organização execute um processo de Gerenciamento de Configuração e Ativos de Serviço, de modo a fornecer o gerenciamento e o controle sobre ativos de TI da organização. Ela orienta ainda que seja criado e mantido uma base de dados do gerenciamento de configuração que contenha informações precisas que possam alimentar outros processos da ITIL.

Para os itens i) e j) do Quadro 5, a ITIL orienta que a organização execute um processo de Gerenciamento de Liberação e Implantação, de modo a proteger o ambiente de produção em caso de mudança *software* ou *hardware* com a execução de procedimentos formais ou testes para verificar se a mudança possui falhas. Esse processo deve incluir fatores como o gerenciamento, distribuição e implementação de *software* e *hardware* aprovados, garantir que apenas versões autorizadas que foram aprovados no processo de qualidade sejam

utilizadas nos ambientes de teste e produção e garantir um armazenamento seguro de *software* e *hardware*.

Para os itens k) e l) do Quadro 5, a ITIL orienta que a organização realize o Gerenciamento de Incidentes, de modo a recuperar os serviços o mais breve possível com o menor impacto negativo. Ela demonstra que esse gerenciamento mantém os usuários informados sobre seu andamento, realiza avaliação e comunica quais as possíveis causas do incidente e identifica os principais incidentes para que os mesmos sejam tratados com maior urgência e com menor prazo de resposta. A pessoa responsável pela gerencia dos incidentes deve desenvolver e tornar seus processos mais eficientes, documentar os incidentes e gerenciar a equipe de resposta ao tratamento. Além de servir de base para o Gerenciamento de Problemas.

Para os itens m) e n) do Quadro 5, a ITIL orienta que a organização realize o Gerenciamento de Problemas, de modo a evitar que os problemas reincidentes gerem indisponibilidade nos serviços diminuindo sua produtividade. Ou seja, utiliza-se de uma abordagem proativa na qual tenta eliminar por definitivo este problema, visto que o Gerenciamento de Incidentes usa uma abordagem reativa que foca em tornar os serviços disponíveis o mais rápido possível, sem se preocupar com sua reincidência. O Gerenciamento de Problemas deve possuir uma base de dados de erros conhecidos que é alimentada tanto pelo Gerenciamento Incidentes quanto pela experiência adquirida pelo tratamento de novos problemas desconhecidos. Ele também deve trabalhar paralelamente com o Gerenciamento de Mudança, de modo que as correções realizadas sejam definitivas e não gerem novos erros. A pessoa responsável por este gerenciamento, deve acompanhar a equipe de resolução de problemas, garantir a integridade da base de erros conhecidos e monitorar todas as atividades de revisão dos problemas.

4.2 GERENCIAMENTO DE NÍVEL DE SERVIÇO DE TI

Nesta seção as boas práticas identificadas são a NBR ISO/IEC 20000-2 e a ITIL. Estas mesmas tratam de seis itens, conforme demonstrado o relacionamento entre eles e as práticas no Quadro 6.

Quadro 6 - Boas práticas para Gerenciamento de Nível de Serviço de TI.

Item	NBR ISO/IEC 20000-2	ITIL
a) a organização mantém um catálogo publicado e atualizado dos serviços de TI oferecidos às áreas clientes, incluindo os níveis de serviço definidos.	Capítulo: 6.1.3.2 Catálogo de serviços	Não se aplica
b) os níveis de serviço são formalmente definidos entre a área de TI e as áreas clientes (Acordo de Nível de Serviço - ANS).	Capítulo: 6.1.3.3 Acordos de Nível de Serviço	Service Design Capítulo: 4.2 Gerenciamento de Nível de Serviço Capítulo: 4.2.5 Atividades, Métodos e Técnicas do Processo
c) os ANS incluem, como indicador de nível de serviço, o grau de satisfação dos usuários, apurado mediante a avaliação dos serviços de TI pelas áreas clientes.	Capítulo: 6.1.2 O processo de gerenciamento do nível de serviços	Service Design Capítulo: 4.2 Gerenciamento de Nível de Serviço Capítulo: 4.2.5 Atividades, Métodos e Técnicas do Processo
d) a área de TI monitora o alcance dos níveis de serviço definidos.	Capítulo: 6.1.2 O processo de gerenciamento do nível de serviços 6.1.3.3 Acordos de Nível de Serviço	Service Design Capítulo: 4.2 Gerenciamento de Nível de Serviço. Capítulo: 4.2.5 Atividades, Métodos e Técnicas do Processo
e) a área de TI implementa ações corretivas em caso de não alcance dos níveis de serviço definidos.	Capítulo: 6.1.3.3 Acordos de Nível de Serviço	Service Design Capítulo: 4.2 Gerenciamento de Nível de Serviço Capítulo: 4.2.5 Atividades, Métodos e Técnicas do Processo
f) a área de TI comunica periodicamente o resultado desse monitoramento às áreas clientes.	Capítulo: 6.1.2 O processo de gerenciamento do nível de serviços	Service Design Capítulo: 4.2 Gerenciamento de Nível de Serviço Capítulo: 4.2.5 Atividades, Métodos e Técnicas do Processo

Fonte: Os Autores, 2017.

Para o item a) do Quadro 6, a NBR ISO/IEC 20000-2 orienta a obrigatoriedade da criação, atualização contínua e disponibilidade aos interessados de um catálogo de serviços, em que o mesmo deve possuir linguagem comum, não exigindo conhecimento técnico detalhado para sua compreensão. Além de propor que a descrição dos serviços existentes seja objetiva e relevante à atividade. Ele também deve ser constituído de atributos considerados necessários para determinada atividade, como de identificação e descrição dos serviços, metas e entre outros.

Para os itens b), d) e e) do Quadro 6, a NBR ISO/IEC 20000-2 orienta a obrigatoriedade da elaboração do Acordo de Nível de Serviço (ANS), o qual deve conter os termos acordados pelo cliente e provedor do serviço, descrição dos serviços e suas metas, especificação das responsabilidades das partes envolvidas, garantias a entrega do serviço e o cumprimento das metas específicas pelo cliente.

Para os itens c), d) e f) do Quadro 6, a NBR ISO/IEC 20000-2 orienta a obrigatoriedade da criação de um processo de Gerenciamento de Nível de Serviço, o qual deve definir, acordar, documentar, monitorar, reportar e analisar criticamente a entrega dos serviços. Além de tornar necessário a existência de uma interação e aproximação entre o negócio e seus fornecedores, com o objetivo de garantir que as necessidades do negócio sejam atendidas.

Para os itens b), c), d) e e) f) do Quadro 6, a ITIL divide o Gerenciamento de Nível de Serviço em 5 atividades chave do processo. Sendo elas: a) o planejamento do ANS; b) acompanhamento do serviço; c) aceitação do serviço pelo mercado; d) avaliar a execução do serviço; e e) propor ações corretivas no ANS.

4.3 GESTÃO DE RISCO DE TI

Nesta seção as boas práticas identificadas são a NBR ISO/IEC 38500, COBIT 5 e a NBR ISO 31000. Estas mesmas tratam de cinco itens, conforme demonstrado o relacionamento entre eles e as práticas no Quadro 7 e 8.

Quadro 7 - Boas práticas para Gestão de Riscos de TI, parte 1.

Item	NBR ISO/IEC 38500	COBIT 5
a) a organização identifica os riscos de TI dos processos críticos de negócio.	Capítulo: 3.7 Princípio 6: Comportamento Humano. Dirigir	APO12.01 Coletar dados
b) a organização avalia os riscos de TI dos processos críticos de negócio.	Capítulo: 3.5 Princípio 4: Desempenho. Avaliar Capítulo: 3.3 Princípio 2: Estratégia. Avaliar	APO12.02 Analisar riscos
c) a organização trata os riscos de TI dos processos críticos de negócio com base em um plano de tratamento de risco.	Não se aplica	APO12.03 Manter um perfil de risco APO12.04 Comunicar risco APO12.05 Definir um portfólio de ações para gerenciamento de risco APO12.06 Responder aos riscos
d) a organização executa um processo de gestão de riscos de TI.	Capítulo: 3.7 Princípio 6: Comportamento Humano. Dirigir	APO12.03 Manter um perfil de risco APO12.04 Comunicar risco APO12.05 Definir um portfólio de ações para gerenciamento de risco
e) o processo de gestão de riscos de TI está formalmente instituído, como norma de cumprimento obrigatório.	Não se aplica	APO12 Gestão de riscos

Fonte: Os Autores, 2017.

Quadro 8 - Boas práticas para Gestão de Riscos de TI, parte 2.

Item	NBR ISO 31000
a) a organização identifica os riscos de TI dos processos críticos de negócio.	Capítulo: 5.4.2 Identificação de riscos
b) a organização avalia os riscos de TI dos processos críticos de negócio.	Capítulo: 5.4.4 Avaliação de riscos
c) a organização trata os riscos de TI dos processos críticos de negócio com base em um plano de tratamento de risco.	Capítulo: 5.5 Tratamento de riscos
d) a organização executa um processo de gestão de riscos de TI.	Capítulo: 5 Processo
e) o processo de gestão de riscos de TI está formalmente instituído, como norma de cumprimento obrigatório.	Capítulo: 4.3.2 Estabelecimento da Política de Gestão de Riscos Capítulo: 4.3.3 Responsabilização

Fonte: Os Autores, 2017.

Para os itens a) e d) do Quadro 7, a NBR ISO/IEC 38500 identifica a necessidade do gerenciamento dos riscos, conforme as políticas e procedimentos definidos pela organização. Além de orientar que é de responsabilidade dos gestores ou responsáveis da organização, exigir que a identificação e comunicação dos riscos de TI possa ser realizada por qualquer colaborador e a qualquer momento.

Para o item b) do Quadro 7, a NBR ISO/IEC 38500 orienta que é de responsabilidade dos gerentes de TI da organização analisar e avaliar os riscos à continuidade da atividade de TI, à integridade da informação e proteção dos ativos de TI, em conformidade com normas nacionais e internacionais.

Para os itens a) e b) do Quadro 7, o COBIT 5 orienta a necessidade da comunicação dos riscos, porém para tal atividade é necessário que seja realizada a identificação e coleta dos dados relevantes aos riscos de TI. A avaliação dos riscos viabiliza uma melhor tomada de decisão, permitindo a continuidade na execução das atividades de TI.

Para os itens c) e d) do Quadro 7, o COBIT 5 orienta a necessidade de criar e manter um inventário de riscos, o qual deve conter atributos referentes ao risco e suas contingências. Para que seja possível responder ou atuar adequadamente a curto prazo, com intuito de controlar e limitar o impacto negativo à organização ou aproveitar oportunidades em níveis aceitáveis de risco.

Para o item e) do Quadro 7, o COBIT 5 orienta que seja realizada a gestão dos riscos de TI, por meio da identificação, avaliação e redução dos riscos a um nível aceitável, para que seja possível equilibrar o custo benefício da realização da gestão de riscos de TI. Estes vistos nas orientações referentes aos itens a), b), c) e d).

Para o item a) do Quadro 8, a NBR ISO 31000 orienta que a organização faça uso de ferramentas e técnicas de identificação de riscos de modo a compor uma lista de riscos que

possam impactar a realização dos objetivos organizacionais. Essa lista deve conter as fontes de risco, áreas de impactos, eventos e suas causas e consequências potenciais.

Para o item b) do Quadro 8, a NBR ISO 31000 orienta que seja realizada a avaliação dos riscos classificando e ordenando pela prioridade quais potenciais riscos necessitam de tratamento. As decisões tomadas no processo de avaliação precisam estar em conformidade com critérios e requisitos legais.

Para o item c) do Quadro 8, a NBR ISO 31000 orienta que a seleção do tratamento seja realizada levando em consideração se os esforços e custos provenientes do tratamento do risco são economicamente viáveis, conforme fatores regulamentares e legais. Entre as opções de tratamento do risco estão: não iniciar qualquer atividade que possa causar algum risco; avaliar se determinado risco compensa perante determinada oportunidade; eliminar a fonte do risco; e entre outros.

Para o item d) do Quadro 8, a NBR ISO 31000 orienta que seja elaborado um processo cíclico. No qual é realizado a análise e a avaliação do risco, identificando quais riscos não são tolerados e necessitam de tratamento, conforme item b) e a implementação de um plano de tratamento de riscos e uma posterior avaliação dos resultados do tratamento do risco, conforme item c). Na avaliação dos resultados deverá ser verificada a efetividade do tratamento e se o tratamento gerou algum novo risco.

Para o item e) do Quadro 8, a NBR ISO 31000 orienta que na política de gestão de riscos estabeleça a obrigatoriedade do comprometimento e responsabilização da organização, no que se refere a gestão de risco, atribuindo responsabilidades para o gerenciamento.

4.4 GESTÃO CORPORATIVA DA SEGURANÇA DA INFORMAÇÃO

Nesta seção as boas práticas identificadas são a NBR ISO/IEC 27001, 27002 e 27005. Esta mesma trata de vinte e um itens, conforme demonstrado o relacionamento entre eles e a prática no Quadro 9 e 10.

Quadro 9 - Boas práticas de Gestão Corporativa da Segurança da Informação, parte 1.

Item	NBR ISO/IEC 27001	NBR ISO/IEC 27002
a) a organização dispõe de uma política de segurança da informação formalmente instituída, como norma de cumprimento obrigatório.	Capítulo: 4 Sistema de gestão de segurança da informação	Capítulo: 5 Política de segurança de informação

Quadro 9 - Boas práticas de Gestão Corporativa da Segurança da Informação, continuação parte 1.

b) a organização dispõe de comitê de segurança da informação formalmente instituído, responsável por formular e conduzir diretrizes para a segurança da informação corporativa, composto por representantes de áreas relevantes da organização.	Não se aplica	Capítulo: 6.1 Organização interna
c) a organização possui gestor de segurança da informação formalmente designado, responsável pelas ações corporativas de segurança da informação.	Não se aplica	Capítulo: 6.1.3 Atribuição de responsabilidades para a segurança da informação
d) a organização dispõe de política de controle de acesso à informação e aos recursos e serviços de TI formalmente instituída, como norma de cumprimento obrigatório.	Não se aplica	Capítulo: 11 Controle de Acesso
e) a organização dispõe de política de cópias de segurança (backup) formalmente instituída, como norma de cumprimento obrigatório.	Não se aplica	Capítulo: 10.5 Cópias de segurança
f) a organização executa processo de gestão de ativos, assegurando a definição de responsabilidades e a manutenção de inventário dos ativos.	Não se aplica	Capítulo: 7.1 Responsabilidades pelos ativos
g) o processo de gestão de ativos está formalmente instituído, como norma de cumprimento obrigatório.	Não se aplica	Capítulo: 7 Gestão de ativos
h) a organização executa processo para classificação e tratamento de informações.	Não se aplica	Capítulo: 7.2 Classificação da informação
i) o processo para classificação e tratamento de informações está formalmente instituído, como norma de cumprimento obrigatório.	Não se aplica	Capítulo: 7.2 Classificação da informação
j) a organização implementa controles para garantir a proteção adequada ao grau de confidencialidade de cada classe de informação.	Não se aplica	Capítulo: 7.2.2 Rótulos e tratamento da informação
k) a organização executa processo de gestão de riscos de segurança da informação.	Não se aplica	Não se aplica
l) o processo de gestão de riscos de segurança da informação está formalmente instituído, como norma de cumprimento obrigatório.	Não se aplica	Não se aplica
m) a organização executa processo de gestão de vulnerabilidades técnicas de TI, com objetivo de reduzir o risco de exploração de vulnerabilidades conhecidas.	Não se aplica	Capítulo: 12.6 Gestão de vulnerabilidades técnicas
n) o processo de gestão de vulnerabilidades técnicas de TI está formalmente instituído, como norma de cumprimento obrigatório.	Não se aplica	Capítulo: 12.6 Gestão de vulnerabilidades técnicas

Quadro 9 - Boas práticas de Gestão Corporativa da Segurança da Informação, continuação parte 1.

o) organização executa processo de monitoramento do uso dos recursos de TI, com objetivo de detectar atividades não autorizadas.	Não se aplica	Capítulo: 10.10 Monitoramento
p) o processo de monitoramento do uso dos recursos de TI está formalmente instituído, como norma de cumprimento obrigatório.	Capítulo: 4.2.3 Monitorar e analisar criticamente o SGSI	Capítulo: 10.10 Monitoramento
q) a organização executa processo de gestão de incidentes de segurança da informação.	Capítulo: 4.2.3 Monitorar e analisar criticamente o SGSI	Capítulo: 13 Gestão de incidentes de segurança da informação
r) o processo de gestão de incidentes de segurança da informação está formalmente instituído, como norma de cumprimento obrigatório.	Capítulo: 4.2.3 Monitorar e analisar criticamente o SGSI	Capítulo: 13 Gestão de incidentes de segurança da informação
s) a organização possui equipe de tratamento e resposta a incidentes de segurança em redes computacionais, formalmente instituída.	Capítulo: 4.2.3 Monitorar e analisar criticamente o SGSI	Capítulo: 13 Gestão de incidentes de segurança da informação
t) a organização realiza, de forma periódica, ações de conscientização, educação e treinamento em segurança da informação para seus colaboradores.	Capítulo: 5.2.2 Treinamento, conscientização e competência	Capítulo: 8.2.2 Conscientização, educação e treinamento em segurança da informação
u) a organização utiliza sistema criptográfico, aderente ao processo de certificação digital da ICP-Brasil, para garantir a autenticidade (autoria e integridade) das informações.	Não se aplica	Capítulo: 12.3 Controles criptográficos

Fonte: Os Autores, 2017.

Quadro 10 - Boas práticas de Gestão Corporativa da Segurança da Informação, parte 2.

Item	NBR ISO/IEC 27005
a) a organização dispõe de uma política de segurança da informação formalmente instituída, como norma de cumprimento obrigatório.	Não se aplica
b) a organização dispõe de comitê de segurança da informação formalmente instituído, responsável por formular e conduzir diretrizes para a segurança da informação corporativa, composto por representantes de áreas relevantes da organização.	Não se aplica
c) a organização possui gestor de segurança da informação formalmente designado, responsável pelas ações corporativas de segurança da informação.	Não se aplica
d) a organização dispõe de política de controle de acesso à informação e aos recursos e serviços de TI formalmente instituída, como norma de cumprimento obrigatório.	Não se aplica
e) a organização dispõe de política de cópias de segurança (backup) formalmente instituída, como norma de cumprimento obrigatório.	Não se aplica
f) a organização executa processo de gestão de ativos, assegurando a definição de responsabilidades e a manutenção de inventário dos ativos.	Não se aplica
g) o processo de gestão de ativos está formalmente instituído, como norma de cumprimento obrigatório.	Não se aplica

Quadro 10 - Boas práticas de Gestão Corporativa da Segurança da Informação, continuação parte 2.

h) a organização executa processo para classificação e tratamento de informações.	Não se aplica
i) o processo para classificação e tratamento de informações está formalmente instituído, como norma de cumprimento obrigatório.	Não se aplica
j) a organização implementa controles para garantir a proteção adequada ao grau de confidencialidade de cada classe de informação.	Não se aplica
k) a organização executa processo de gestão de riscos de segurança da informação.	Capítulo: 6 Visão geral do processo de gestão de riscos de segurança da informação
l) o processo de gestão de riscos de segurança da informação está formalmente instituído, como norma de cumprimento obrigatório.	Capítulo: 7.4 Organização para gestão de riscos de segurança da informação
m) a organização executa processo de gestão de vulnerabilidades técnicas de TI, com objetivo de reduzir o risco de exploração de vulnerabilidades conhecidas.	Não se aplica
n) o processo de gestão de vulnerabilidades técnicas de TI está formalmente instituído, como norma de cumprimento obrigatório.	Não se aplica
o) organização executa processo de monitoramento do uso dos recursos de TI, com objetivo de detectar atividades não autorizadas.	Não se aplica
p) o processo de monitoramento do uso dos recursos de TI está formalmente instituído, como norma de cumprimento obrigatório.	Não se aplica
q) a organização executa processo de gestão de incidentes de segurança da informação.	Não se aplica
r) o processo de gestão de incidentes de segurança da informação está formalmente instituído, como norma de cumprimento obrigatório.	Não se aplica
s) a organização possui equipe de tratamento e resposta a incidentes de segurança em redes computacionais, formalmente instituída.	Não se aplica
t) a organização realiza, de forma periódica, ações de conscientização, educação e treinamento em segurança da informação para seus colaboradores.	Não se aplica
u) a organização utiliza sistema criptográfico, aderente ao processo de certificação digital da ICP-Brasil, para garantir a autenticidade (autoria e integridade) das informações.	Não se aplica

Fonte: Os Autores, 2017.

Para o item a) do Quadro 9, a NBR ISO/IEC 27001 orienta que uma política de segurança da informação seja implementada e mantida, monitorada, melhorada continuamente dentro do contexto das atividades de negócio globais da organização afim de enfrentar os riscos aos quais ela pode estar sujeita.

Para os itens p), q), r) e s) do Quadro 9, a NBR ISO/27001 orienta que a organização execute procedimentos de monitoramento e análise crítica para detectar erros nos resultados de processamento, identificar tentativas e violações de segurança, ajudar a detectar e prevenir incidentes de segurança da informação, determinar se ações realizadas para solucionar uma violação de segurança foram eficazes e permite que a direção verifique se as pessoas responsáveis pelas atividades de segurança da informação estão executando os procedimentos conforme o esperado.

Para o item t) do Quadro 9, a NBR ISO/IEC 27001 orienta que a organização mantenha, forneça, execute e monitore ações de conscientização ou treinamentos, afim de verificar sua eficiência e assegurar que os colaboradores estejam conscientes de sua importância e que eles contribuam para seu alcance.

Para o item a) do Quadro 9, a NBR ISO/IEC 27002 orienta que a organização crie e mantenha atualizado um conjunto de políticas de segurança da informação, sendo está aprovada pela sua gestão. Os gestores devem comunicar e tornar acessível a todos os funcionários estas políticas. As políticas devem conter aspectos relativos a: sua definição, metas, escopo, importância, comprometido da direção, princípios, sua estrutura, os objetivos, os controles, as conformidades legais e regulamentares, e devem estar em conformidade com os requisitos do negócio.

Para os itens b) e c) do Quadro 9, a NBR ISO/IEC 27002 orienta que seja estabelecido dentro da organização uma estrutura gerencial para controlar e operar as atividades da segurança da informação, e que seja definido e atribuindo os papéis e as responsabilidades pela segurança da informação a um gestor ou equipe capacitada, conforme a política de segurança da informação.

Para o item d) do Quadro 9, a NBR ISO/IEC 27002 orienta que a organização possua, documente e dissemine uma política de controle de acesso à informação e aos ativos de TI entre seus colaboradores e que está esteja aderente aos requisitos do negócio e da política de segurança da informação. Esta política de controle de acesso deve considerar fatores físicos e lógicos da organização e deve ser mantida atualizada.

Para o item e) do Quadro 9, a NBR ISO/IEC 27002 orienta que a organização possua uma política de geração de cópias de segurança, de modo a garantir a integridade e disponibilidade das informações em caso de desastre ou falha. Ela define ainda, que esta política deve ser efetuada e testada regularmente de modo a garantir que toda a informação e *softwares* estarão disponíveis caso necessite de recuperação. Ela indica ainda parâmetros que possam assegurar a validade desta política como: o que deve conter nas cópias de segurança, frequência de geração das cópias, local de armazenamento, testes dos recursos utilizados para geração das cópias, procedimentos para recuperação, entre outros.

Para os itens f) e g) do Quadro 9, a NBR ISO/IEC 27002 orienta que a organização possua e mantenha atualizado um inventário de ativos, que todos os ativos estejam identificados e contidos nesse inventário, de modo a possuir um proprietário responsável a quem será delegada a responsabilidade pela proteção e manutenção apropriada.

Para os itens h), i) e j) do Quadro 9, a NBR ISO/IEC 27002 orienta que a informação seja classificada adequadamente por meio de um sistema de classificação da informação, indicando a necessidade, prioridade e o nível de proteção adequado, variando entre seu valor, os níveis de sensibilidade e criticidade e os requisitos legais podendo necessitar de um nível de proteção ou tratamento especial. Orienta também que seja definido e implementado um conjunto apropriado de procedimentos para a rotulação e tratamento da informação que abranja tanto os ativos de informação no formato físico quanto eletrônico, devendo definir todos os seus procedimentos de forma adequada, como: processamento seguro, armazenagem, transmissão e compartilhamento, reclassificação e destruição.

Para os itens m) e n) do Quadro 9, a NBR ISO/IEC 27002 orienta que a gestão de vulnerabilidades técnicas seja implementada e monitorada regularmente de forma efetiva, sistemática e repetível com medições que confirmem a sua efetividade, com o objetivo de reduzir riscos resultantes de vulnerabilidades técnicas já conhecidas pela comunidade, abrangendo os sistemas operacionais e quaisquer aplicações utilizadas pela organização.

Para os itens o) e p) do Quadro 9, a NBR ISO/IEC 27002 orienta que a organização estabeleça que os sistemas sejam monitorados e que eventos de segurança da informação como tentativas de invasão sejam registrados, com o objetivo de detectar atividades não autorizadas de processamento da informação. Registros de operador e de falhas devem ser utilizados para assegurar a identificação de problemas nos sistemas de informação. Os registros de auditoria que contém as atividades dos usuários e outros eventos de segurança devem ser mantidos conforme período de tempo definido pela política de segurança da informação da organização.

Para os itens q), r) e s) do Quadro 9, a NBR ISO/IEC 27002 orienta que a organização estabeleça procedimentos formais de registro e escalonamento para gestão de incidentes de segurança da informação. Orienta também que os funcionários, fornecedores e terceiros estejam comprometidos com os procedimentos de notificação de eventos e fragilidades relacionados com a segurança da informação da organização, devendo notificar ao(s) responsável(is) qualquer evento ocorrido. Após a notificação de qualquer evento, um processo de melhoria continua deve ser aplicado, monitorado e avaliado conforme responsabilidades e procedimentos estabelecidos, assegurando assim respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

Para o item t) do Quadro 9, a NBR ISO/IEC 27002 orienta que a organização forneça a seus funcionários e terceiros treinamento apropriados em conscientização e atualizações regulares nas políticas e procedimentos organizacionais. Orienta também que a

conscientização, educação e treinamento nas atividades de segurança da informação seja realizada conforme as responsabilidades e papéis de cada pessoa, os deixando cientes das ameaças e a forma correta de comunicar os incidentes de segurança da informação presenciados.

Para o item u) do Quadro 9, a NBR ISO/IEC 27002 orienta que a organização desenvolva uma política para o uso de controles criptográficos e que um gerenciamento de chaves seja implementado para apoiar o uso das técnicas de criptografia, com o objetivo de proteger a confidencialidade, a autenticidade ou a integridade das informações. Devem ser consideradas na implementação da política de criptografia as leis e/ou regulamentações e restrições nacionais aplicáveis ao uso de tais técnicas. No desenvolvimento da política devem ser definidos qual nível de proteção, os papéis e responsabilidades, quais padrões adotar e seu impacto de sua utilização.

Para o item k) do Quadro 10, a NBR ISO/IEC 27005 orienta que a organização crie e execute um processo de gestão de riscos de segurança da informação que envolva todos os aspectos da segurança da informação, sendo eles: a definição do contexto, o processo de avaliação de riscos, o tratamento do risco, a aceitação do risco, a comunicação e consulta do risco e o monitoramento e análise crítica de riscos. Ela sugere que os processos de gestão de risco sejam iterativos, permitindo que o processo de avaliação do risco seja melhor detalhado e aprofundado a cada repetição, otimizando o tempo e o esforço utilizado e garantindo uma melhor avaliação para riscos que possam causar um maior impacto negativo na organização.

Para o item l) do Quadro 10, a NBR ISO/IEC 27005 orienta que organização estabeleça e mantenha papéis e responsabilidades para o processo de gestão de riscos de segurança da informação. Entre estes papéis e responsabilidades está o desenvolvimento do processo de gestão de riscos de segurança da informação, estabelecimento das relações necessárias entre a organização e as partes interessadas, bem como a interface com outros projetos e atividades relevantes, definição de parâmetros para a tomada de decisão, especificação de quais registros devem ser mantidos, entre outros.

4.5 PROCESSO DE *SOFTWARE*

Nesta seção a boa prática identificada é a NBR ISO/IEC 12207. Esta mesma trata de cinco itens, conforme demonstrado o relacionamento entre eles e a prática no Quadro 11.

Quadro 11 - Boas práticas de Processo de *Software*.

Item	NBR ISO/IEC 12207
a) a organização executa um processo de <i>software</i> , com o objetivo de assegurar que o <i>software</i> a ser desenvolvido, direta ou indiretamente, atenda às suas necessidades.	Capítulo: 6 Processo de ciclo de vida de sistema
b) o processo de <i>software</i> é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.	Capítulo: 6 Processo de ciclo de vida de sistema
c) o processo de <i>software</i> é periodicamente revisado e melhorado com base nas mensurações obtidas.	Capítulo: 7.3 Processo de melhoria
d) a organização possui pessoal próprio capacitado para executar o processo de <i>software</i> .	Capítulo: 7.4 Processo de treinamento
e) o processo de <i>software</i> está formalmente instituído, como norma de cumprimento obrigatório.	Capítulo: 5 Processos fundamentais de ciclo de vida

Fonte: Os Autores, 2017.

Para os itens a) e b) do Quadro 11, a NBR ISO/IEC 12207 orienta que a organização deva possuir um processo de *software* com pessoas responsáveis por verificar e assegurar que ele atenda às necessidades solicitadas, de modo a garantir a qualidade do produto e a consistência conforme consta no contrato. Ela orienta ainda que devam ser realizadas atividades de revisões conjuntas, auditorias, verificações e validações de modo a garantir qualidade do produto.

Para o item c) do Quadro 11, a NBR ISO/IEC 12207 orienta que a organização estabeleça procedimentos para melhoria dos processos. Que consiste em monitor e avaliar o processo, documentar os dados obtidos, executar revisões quando necessário para garantir sua contínua adequação e eficiência, levando em consideração os resultados da avaliação.

Para o item d) do Quadro 11, a NBR ISO/IEC 12207 orienta que a organização realize treinamentos com o pessoal do desenvolvimento de *software*, de modo a mantê-los sempre qualificados. Ela orienta ainda que os treinamentos sejam planejados e implementados antecipadamente, para que o pessoal qualificado esteja disponível quando o produto de *software* for passar por melhorias ou correções. Ela indica ainda que seja criado um plano de treinamento, manuais de treinamento e a posterior implementação do treinamento, documentando todo o processo.

Para o item e) do Quadro 11, a NBR ISO/IEC 12207 orienta seja mantido um processo fundamental, para garantir a existência e funcionamento do processo de desenvolvimento de *software*, sendo de responsabilidade da organização a fiscalização.

4.6 GERENCIAMENTO DE PROJETOS DE TI

Nesta seção as boas práticas identificadas são o COBIT 5 e o PMBOK. Esta mesma trata seis itens, conforme demonstrado o relacionamento entre eles e a prática no Quadro 12.

Quadro 12 - Boas práticas de Gerenciamento de Projetos de TI.

Item	COBIT 5	PMBOK
a) a organização possui portfólio de projetos de TI.	BAI01 Gerenciar programas e Projetos	Capítulo: 1.4 Relacionamentos entre gerenciamento de portfólios, gerenciamento de programas, gerenciamento de projeto e gerenciamento organizacional de projetos
b) a organização executa processo de gerenciamento de projetos de TI.	BAI01.07 Iniciar projetos dentro de um programa BAI01.08 Planejar projetos	Capítulo: 1.3 O que é gerenciamento de projetos?
c) o processo de gerenciamento de projetos de TI é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.	BAI01.11 Monitorar e controlar projetos	Capítulo: 1.4 Relacionamentos entre gerenciamento de portfólios, gerenciamento de programas, gerenciamento de projeto e gerenciamento organizacional de projetos
d) o processo de gerenciamento de projetos de TI é periodicamente revisado e melhorado com base nas mensurações obtidas.	BAI01.13 Finalizar um projeto	Capítulo: 3.6 Grupo de processos de monitoramento e controle
e) o processo de gerenciamento de projetos de TI está formalmente instituído, como norma de cumprimento obrigatório.	BAI01.08 Planejar projetos	Capítulo: 1.3 O que é gerenciamento de projetos Capítulo: 3 Processos de gerenciamento de projetos
f) a organização possui um escritório de projetos, ao menos para projetos de TI.	BAI01.05 Inicie e execute o programa	Capítulo: 1.4.4 Escritório de gerenciamento de projetos

Fonte: Os Autores, 2017.

Para o item a) do Quadro 12, o COBIT 5 orienta que a organização realize o Gerenciamento de Portfólio, de modo que todos os projetos e programas sejam planejados, iniciados, executados, alinhados e coordenados com os objetivos e estratégias da organização. Esse gerenciamento permite a redução dos riscos de atrasos inesperados, custo, perda de valor e melhora a comunicação entre os *stakeholders*, com intuito de maximizar seu o valor e sua qualidade.

Para os itens b) e e) do Quadro 12, o COBIT 5 orienta que a organização defina formalmente um plano de Gerenciamento de Projetos de TI, de modo a definir e documentar claramente o escopo e a natureza do projeto. O gerenciamento torna possível o entendimento comum do projeto entre as partes interessadas, a comunicação entre outros projetos da organização e a execução e controle ao longo de todo o ciclo de vida do projeto. Ele orienta

também que esse plano deva ser aprovado pela alta administração da organização antes de entrar em produção.

Para os itens c) e d) do Quadro 12, o COBIT 5 orienta que a organização realize uma medição do desempenho dos projetos utilizando métricas como: prazo, qualidade, custo e risco e deve comunicar os gerentes os impactos dos desvios identificados. Orienta também que ao final de cada projeto os resultados sejam analisados para verificar se alcançou o objetivo planejado, documentando todos os pontos que não atingiram seus objetivos e as novas lições aprendidas para que sejam utilizados em projetos futuros.

Para o item f) do Quadro 12, o COBIT 5 orienta que após planejar, estabelecer, realizar e gerenciar as etapas referentes a criação do projeto, deve ser configurado um escritório de gerenciamento de projetos, de modo a dar suporte à execução dos projetos.

Para o item a) do Quadro 12, o PMBOK orienta que seja realizado o gerenciamento de portfólio, para que por meio dele os projetos ou programas com maior importância recebam a devida atenção e recursos necessários, otimizando o uso dos recursos de modo a auxiliar a atingir a estratégia organizacional.

Para o item b) do Quadro 12, o PKBOK orienta que o seja desenvolvido um plano de gerenciamento de projetos de forma interativa ao longo de todo o ciclo de vida do projeto, e que seja realizada a melhoria contínua por meio dos dados obtidos sobre o projeto ao longo dele, permitindo que sua equipe tenha maior precisão no gerenciamento dos projetos.

Para o item c) do Quadro 12, o PMBOK orienta que sejam implementadas métricas de modo a garantir sucesso do gerenciamento de projetos por meio de medição qualidade do produto ou do projeto, pela pontualidade, pelo cumprimento do orçamento e pelo grau de satisfação dos *stakeholders*.

Para o item d) do Quadro 12, o PKBOK orienta que os dados obtidos a parte do item c) sejam monitorados continuamente pela equipe de gerenciamento de projetos, para que mudanças e ações corretivas ou preventivas sejam recomendadas caso necessário, de modo a antecipar possíveis problemas, manter a saúde do projeto e identificar áreas que necessitam de maior atenção.

Para o item e) do Quadro 12, o PMBOK orienta que seja instituído formalmente o gerenciamento de projetos, de modo a aumentar a probabilidade de sucesso em seus projetos, concentrando-se na entrega bem-sucedida dos produtos ou serviços, auxiliando a atingir as metas e os objetivos organizacionais.

Para o item f) do Quadro 12, o PMBOK orienta a criação de um escritório de projetos, para entre suas funções, padronizar os processos de governança relacionada a

projetos, permitir o compartilhamento de recursos, ferramentas, técnicas e metodologias. O escritório tem como principal responsabilidade dar apoio ao gerenciamento de projetos e o nível de controle exercido por ele pode variar entre baixo, médio e alto.

4.7 CONTRATAÇÕES DE SERVIÇOS DE TI

Nesta seção a boa prática identificada é o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação. Estas mesmas tratam de nove itens, conforme demonstrado o relacionamento entre eles e as práticas no Quadro 13.

Quadro 13 - Boas práticas para Contratações de Serviços de TI.

Item	Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação
a) a organização realiza estudos técnicos preliminares para avaliar a viabilidade da contratação.	Capítulo: 6.1 Estudos técnicos preliminares
b) a organização explicita, nos autos, as necessidades de negócio que se pretende atender com a contratação.	Capítulo: 6.1.1 Necessidade da contratação
c) a organização explicita, nos autos, os indicadores dos benefícios de negócio que serão alcançados.	Capítulo: 6.1.10 Resultados pretendidos
d) a organização explicita, nos autos, o alinhamento entre a contratação e os planos estratégico institucional e de TI vigentes.	Capítulo: 6.1.2 Alinhamento entre a contratação e os planos do órgão governante superior, do órgão e de TI do órgão
e) a organização realiza análise dos riscos que possam comprometer o sucesso do processo de contratação e dos resultados que atendam às necessidades de negócio.	Capítulo: 6.1.12 Análise de risco
f) a organização adota métricas objetivas para mensuração de resultados do contrato.	Capítulo: 6.1.10 Resultados pretendidos
g) a organização realiza os pagamentos dos contratos em função da mensuração objetiva dos resultados entregues e aceitos.	Capítulo: 6.3.6 Modelo de gestão do contrato - Item 3
h) a organização realiza a análise dos benefícios reais já obtidos, utilizando-a como critério para prorrogar o contrato.	Capítulo: 6.1.10 Resultados pretendidos
i) a organização diferencia e define formalmente os papéis de gestor e fiscal do contrato.	Capítulo: 6.3.6 Modelo de gestão do contrato - Item 1

Fonte: Os Autores, 2017.

Para o item a) do Quadro 13, o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação orienta que sejam elaborados estudos técnicos preliminares com o objetivo de assegurar a viabilidade técnica da contratação de serviços ou produtos de TI, caso seja considerada viável, eles devem servir como base para execução do plano de trabalho ou projeto básico inicial.

Para o item b) do Quadro 13, o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação orienta a importância de expor as necessidades do negócio, para que sirva de justificativa para a contratação da solução de TI.

Para os itens c), f) e h) do Quadro 13, o Guia de Boas Práticas em Contratação de Soluções de TI orienta que sejam definidos os benefícios esperados pelo órgão com a contratação, podendo ser a eficácia e eficiência na utilização dos recursos ou melhorias na qualidade do serviço prestado. Ele também orienta que sejam estabelecidos os critérios de medições anteriores e posteriores a contratação, possibilitando o acompanhamento dos resultados pretendidos por meio de mensurações.

Para o item d) do Quadro 13, o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação orienta que seja realizado o alinhamento com o objetivo de esclarecer como a solução de TI auxilia no alcance dos objetivos almejados.

Para o item e) do Quadro 13, o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação orienta que seja realizada a análise dos riscos afim de mitigar os riscos identificados ao longo de todo o processo de contratação e gestão do contrato, podendo exigir amostras do serviço ou produto a ser contratado.

Para o item g) do Quadro 13, o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação orienta que sejam estabelecidos critérios de pagamentos que levem em consideração a entrega dos produtos ou serviços contratados após a avaliação dos níveis de serviços entregues ou entrega de etapas de um serviço de acordo com cronograma.

Para o item i) do Quadro 13, o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação orienta que sejam definidos os papéis entre os responsáveis envolvidos com a contratação de serviços ou produtos, de modo que o cargo de gestor pode possuir atribuições de maior responsabilidade, visto que o mesmo deve ter conhecimento gerencial, técnico e operacional. Em contrapartida o fiscal do contrato é uma pessoa responsável apenas pelo acompanhamento e fiscalização do contrato.

4.8 PLANEJAMENTO DAS CONTRATAÇÕES DE TI

Nesta seção a boa prática identificada é o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação. Esta mesma trata de cinco itens, conforme demonstrado o relacionamento entre eles e a prática no Quadro 14.

Quadro 14 - Boas práticas de Planejamento das Contratações de TI.

Item	Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação
a) a organização possui procedimentos internos que auxiliam na padronização das atividades de planejamento das contratações de TI.	Capítulo: 5 Processo de planejamento da contratação de soluções de TI
b) a organização executa processo de planejamento das contratações de TI.	Capítulo: 5 Processo de planejamento da contratação de soluções de TI
c) o processo de planejamento das contratações de TI é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.	Capítulo: 5 Processo de planejamento da contratação de soluções de TI
d) o processo de planejamento das contratações de TI é periodicamente revisado e melhorado com base nas mensurações obtidas.	Capítulo: 5 Processo de planejamento da contratação de soluções de TI
e) o processo de planejamento das contratações está formalmente instituído, como norma de cumprimento obrigatório.	Capítulo: 5 Processo de planejamento da contratação de soluções de TI Capítulo: 8.4 Publicar políticas e normas

Fonte: Os Autores, 2017.

Para os itens a), b), c) e d) do Quadro 14, o Guia de Boas Práticas em Contratação de Soluções de TI compara o planejamento a um projeto, de maneira que ele possua parâmetros bem definidos, que padronize seus processos e que servidores capacitados e com conhecimento técnico sob a aquisição sejam alocados para realizar as contratações, seguindo requisitos legais e de jurisprudência. Orienta ainda a criação de um indicador de prazo médio de conclusão de contratações, para que seja possível definir prazos viáveis em negociações futuras. A qualidade do planejamento está vinculada ao indicador criado e a capacidade dos servidores designados para as contratações.

Para o item e) do Quadro 14, o Guia de Boas Práticas em Contratação de Soluções de TI orienta haja uma modelagem formal do processo de modo a padroniza-lo e possibilitar o aprimoramento do processo. Tornando necessário a formalização, capacitação dos envolvidos e publicação posterior dos resultados de todo o processo aprovado pela alta administração.

4.9 GESTÃO DOS CONTRATOS DE TI

Nesta seção a boa prática identificada é o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação. Esta mesma trata de cinco itens, conforme demonstrado o relacionamento entre eles e as práticas no Quadro 15.

Quadro 15 - Boas práticas de Gestão dos Contratos de TI.

Item	Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação
a) a organização possui procedimentos internos que auxiliam na padronização das atividades de gestão de contratos de TI.	Capítulo: 6.3.6 Modelo de gestão do contrato

Quadro 15 - Boas práticas de Gestão dos Contratos de TI, continuação.

b) a organização executa processo de gestão de contratos de TI.	Capítulo: 6.3.6 Modelo de gestão do contrato
c) o processo de gestão de contratos de TI é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.	Capítulo: 6.3.6 Modelo de gestão do contrato
d) o processo de gestão de contratos de TI é periodicamente revisado e melhorado com base nas mensurações obtidas.	Capítulo: 6.3.6 Modelo de gestão do contrato Capítulo: 8.4 Publicar políticas e normas
e) o processo de gestão de contratos está formalmente instituído, como norma de cumprimento obrigatório.	Capítulo: 6.3.6 Modelo de gestão do contrato Capítulo: 8.4 Publicar políticas e normas

Fonte: Os Autores, 2017.

Para os itens a), b), c), d) e e) do Quadro 15, o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação orienta que os contratos de TI sejam geridos pela área de TI. Ele também orienta que seja feita a verificação do cumprimento das obrigações da contratada ao menos uma vez por ano, definição de critérios para aplicação de sanções em caso de não cumprimento, critérios de qualidade a serem verificados, elaboração de políticas e normas internas que definam os processos e procedimentos da gestão de contratos, possibilitando a sua formalização, o aprimoramento e a reprodução independente do servidor que estiver envolvido.

4.10 PERFIL DAS CONTRATAÇÕES DE TI

Nesta seção não foram sugeridas boas práticas para melhoria do iGovTI, visto que a questão do Perfil das Contratações de Serviço de TI refere-se ao levantamento e acompanhamento dos contratos firmados no ano anterior ao avaliado, conforme observado no Quadro 16.

Quadro 16 - Questões relativas ao Perfil das Contratações de TI.

Item
a) contratações realizadas.
b) contratações que adotaram o sistema de registro de preço (RP), em que a própria organização foi gestora da ata, com participação de outras instituições no planejamento (RP conjunto).
c) contratações que adotaram o sistema de registro de preço, em que a própria organização foi gestora da ata, sem participação de outras instituições no planejamento (RP solitário).
d) contratações que adotaram o sistema de registro de preço, com a participação no planejamento inicial de outra organização, que foi a gestora da ata (participação em RP conjunto).
e) contratações por adesão tardia a ata de registro de preço ("carona"), sem participação no planejamento da contratação
f) contratações por dispensa de licitação por contrato emergencial.
g) contratações por dispensa de licitação para contratar órgão/entidade da Administração Pública (Lei 8.666/1993, art. 24, VII ou XVI).
h) contratações por inexigibilidade de licitação.

Fonte: TCU (2016).

4.11 VISÃO GERAL

Nas seções 4.1 a 4.10 foram apresentados o direcionamento e a análise de cada uma das boas práticas de GovTIC para cada temática da dimensão de Processos.

Os Quadros apresentados no neste capítulo indica o direcionamento, demonstrando para cada item de uma determinada temática qual capítulo, apêndice, seção ou tópico das boas práticas selecionadas que a abordam. Esse direcionamento pode auxiliar os gestores a identificar o local onde buscar orientações na implementação das melhorias de Governança.



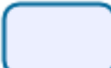




Já a análise das boas práticas de GovTIC é uma apresentação de forma resumida do que as boas práticas orientam e sugerem para atender cada item do questionário que aborda as temáticas da dimensão de Processos. A apresentação dessa análise pode ser utilizada como uma forma de incentivar os gestores a iniciar ou melhorar a implementação das boas práticas.

5 MODELO DE PROCESSOS DAS BOAS PRÁTICAS

Neste capítulo é apresentado os modelos de processo BPM que foram elaborados com base na análise das boas práticas apresentadas no capítulo 4. Por meio de tais modelos as organizações que fazem parte da APF poderão guiar-se na implementação das boas práticas apresentadas neste trabalho com o objetivo de melhorar o nível de maturidade do iGovTI.

No Quadro 17 é apresentado a descrição de cada símbolo utilizado para desenvolver o modelo de processos BPM.

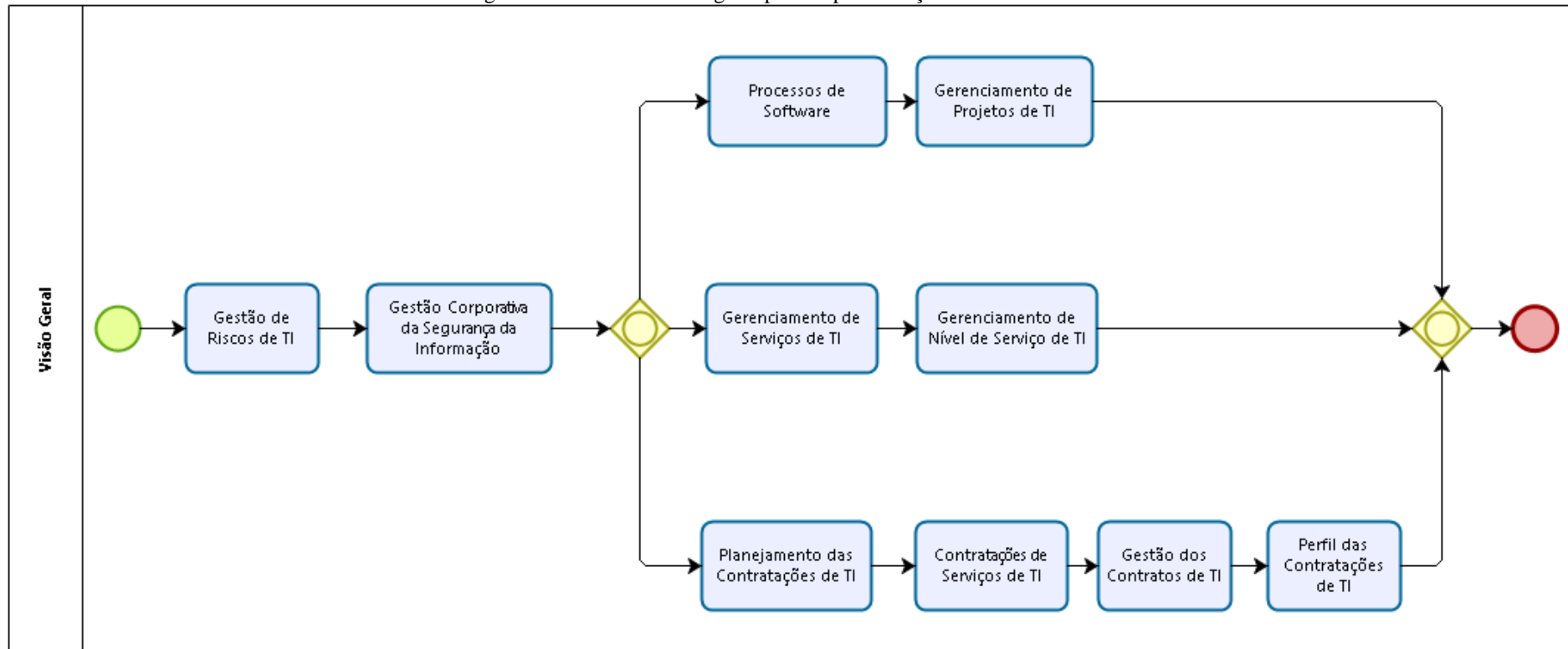
Quadro 17 - Dicionário de Símbolos BPM utilizando o Bizagi.

Símbolo	Descrição
	Evento de início que indica onde um processo começará.
	Evento de fim que indica onde o processo terminará.
	Tarefa que indica uma atividade atômica que está incluída dentro de um processo.
	Fluxo de Sequência que é usado para mostrar a ordem em que as atividades serão executadas em um processo. Cada fluxo só pode possuir uma origem e um destino.
	Gateways Exclusivos baseado em dados são locais dentro de um processo de negócios no qual o Fluxo de Sequência indica por meio de uma resposta booleana qual caminho único deve ser seguido.
	<i>Gateways</i> Inclusivos são locais dentro de um processo de negócios no qual o Fluxo de Sequência indica por meio de uma resposta booleana qual caminho deve ser seguido, permitindo que múltiplos caminhos sejam seguidos desde satisfaça a condição.
	<i>Gateways</i> Paralelos são locais dentro de um processo de negócios no qual o Fluxo de Sequência que fornece mecanismo para sincronizar e criar o fluxo paralelo, no qual indica que todos os caminhos devem ser seguidos e todas as tarefas realizadas, antes de prosseguir com fluxo normal.

Fonte: Os Autores, 2017.

Um modelo BPM de visão geral de implantação para as boas práticas de GovTIC é apresentado na Figura 3, na qual está relacionado diretamente cada tarefa a uma temática que constituem a dimensão de Processos.

Figura 3 - Modelo de visão geral para Implementação das Boas Práticas.



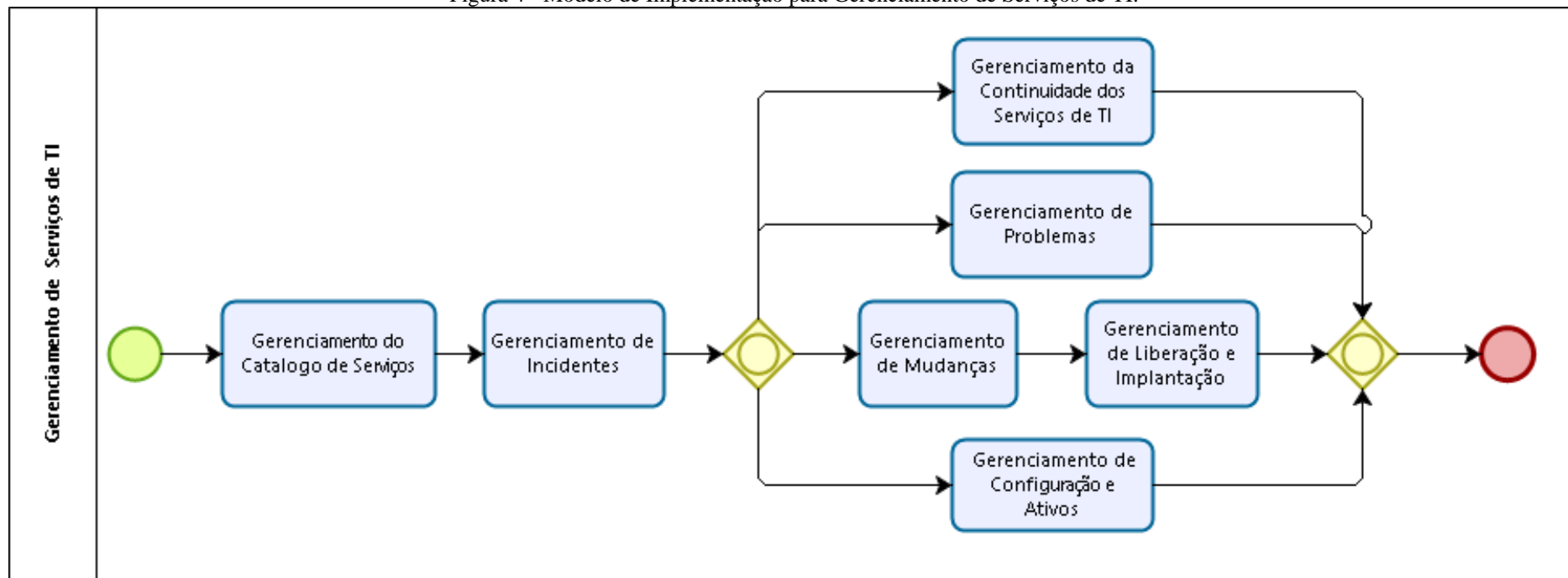
Fonte: Os Autores, 2017.

Nas próximas seções são apresentados os modelos de processo BPM para cada uma das temáticas, correspondendo cada modelo a uma tarefa que compõe o modelo de visão geral, apresentado na Figura 3. O modelo geral está representado em dez tarefas, entretanto, nas próximas seções constam nove modelos BPM, visto que o Perfil das Contratações de TI é referente ao resumo das contratações realizadas no ano anterior a aplicação do questionário do iGovTI pelo TCU.

5.1 GERENCIAMENTO DE SERVIÇOS DE TI

Esta temática está relacionada ao Gerenciamento de Serviços de TI, com o objetivo de catalogar os serviços executados pela organização e garantir a oferta contínua dos serviços com o mínimo de interrupção, mesmo após a ocorrência de incidentes internos e externos, com a implementação do Gerenciamento de Mudanças, de Incidentes e de Problemas. Também visa manter uma base contendo todas as configurações sobre os ativos de TI, para auxiliar o gerenciamento dos ativos de TI da organização. A boa prática que foi utilizada para elaborar o modelo BPM apresentado na Figura 4 é a ITIL.

Figura 4 - Modelo de Implementação para Gerenciamento de Serviços de TI.

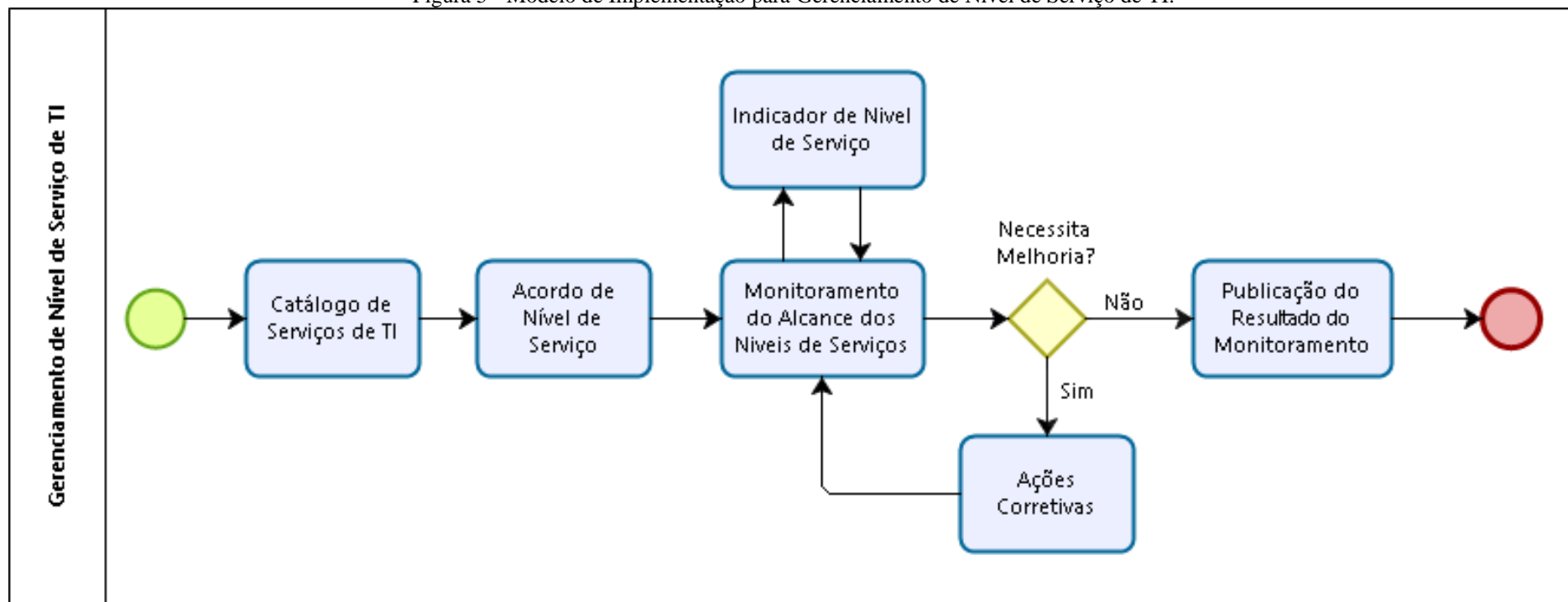


Fonte: Os Autores, 2017.

5.2 GERENCIAMENTO DE NÍVEL DE SERVIÇO DE TI

Esta temática está relacionada ao Gerenciamento de Nível de Serviço de TI, com o objetivo de catalogar os serviços executados pela organização, acompanhar e gerenciar a entrega dos serviços por meio do Gerenciamento de Nível de Serviço. Também define um Acordo de Nível de Serviço contendo os termos acordados nos contratos firmados pelas partes envolvidas. As boas práticas que foram utilizadas para elaborar o modelo BPM apresentado na Figura 5 são a NBR ISO/IEC 20000-2 e a ITIL.

Figura 5 - Modelo de Implementação para Gerenciamento de Nível de Serviço de TI.

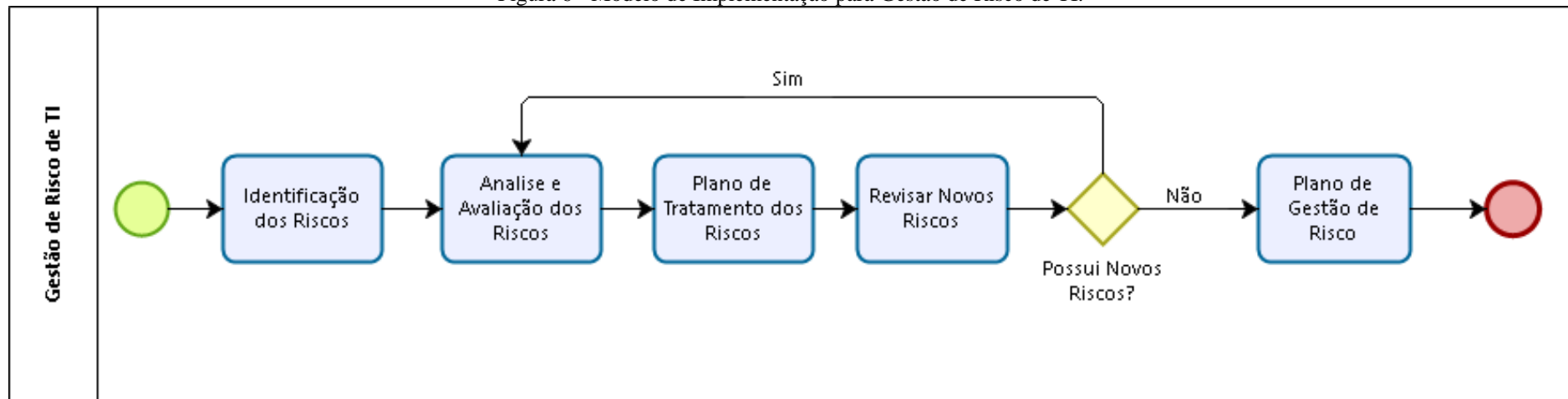


Fonte: Os Autores, 2017.

5.3 GESTÃO DE RISCO DE TI

Esta temática está relacionada à Gestão de Risco de TI, com o objetivo de executar um processo para identificar, analisar, avaliar e definir o tratamento do risco conforme sua gravidade, de modo garantir a continuidade das atividades de TI e mitigar o risco e/ou seu impacto na organização. Além de garantir a integridade da informação e a proteção dos ativos de TI. Ela também propõe atividades que auxiliam a organização a atingir tal objetivo, sendo elas: a melhoria na comunicação interna, a adoção de uma política de gestão de riscos e definir os papéis e as responsabilidades. As boas práticas que foram utilizadas para elaborar o modelo BPM apresentado na Figura 6 são a NBR ISO/IEC 38500, o COBIT 5 e a NBR ISO 31000.

Figura 6 - Modelo de Implementação para Gestão de Risco de TI.

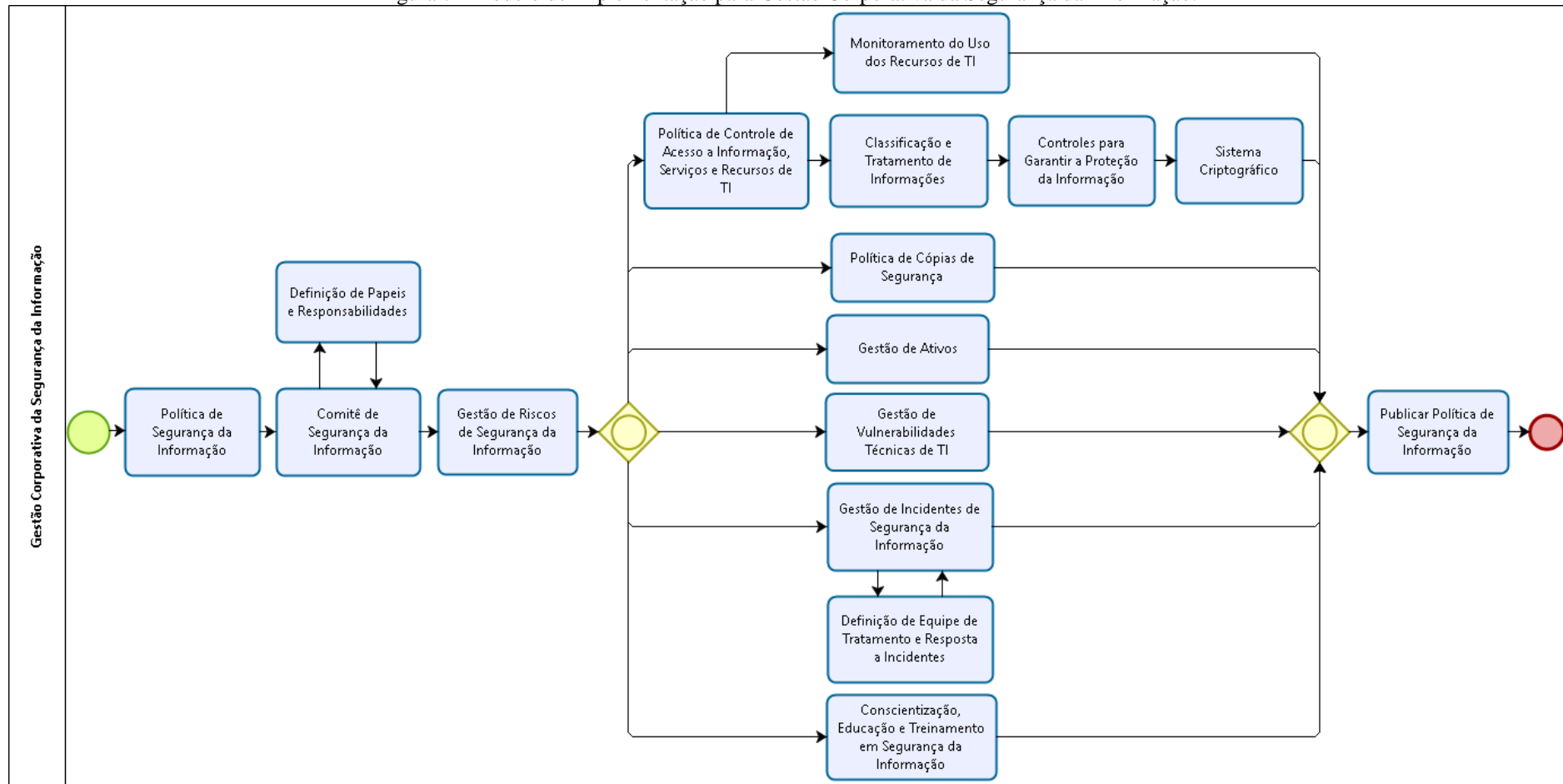


Fonte: Os Autores, 2017.

5.4 GESTÃO CORPORATIVA DA SEGURANÇA DA INFORMAÇÃO

Esta temática está relacionada à Gestão Corporativa da Segurança da Informação, com o objetivo de prevenir, identificar e determinar as ações necessárias para garantir a segurança da informação em caso de invasões e/ou violações. Ela propõe a implementação de um comitê de segurança da informação, de uma política de segurança da informação, de controle de acesso e de cópias de segurança. Além orientar a definição de um processo de Gestão de Riscos de Segurança da Informação, Gestão de Incidentes, Gestão de Ativos, de classificação e tratamento das informações e incluir o uso de sistema criptográfico, de modo a garantir a integridade e confidencialidade da informação. Ela também recomenda que a organização monitore o uso dos recursos de TI e das vulnerabilidades técnicas de TI, possua uma equipe de tratamento e resposta a incidentes e realize ações de conscientização e treinamento sobre segurança da informação. As boas práticas que foram utilizadas para elaborar o modelo BPM apresentado na Figura 7 são a NBR ISO/IEC 27001, a NBR ISO/IEC 27002 e a NBR ISO/IEC 27005.

Figura 7 - Modelo de Implementação para Gestão Corporativa da Segurança da Informação.

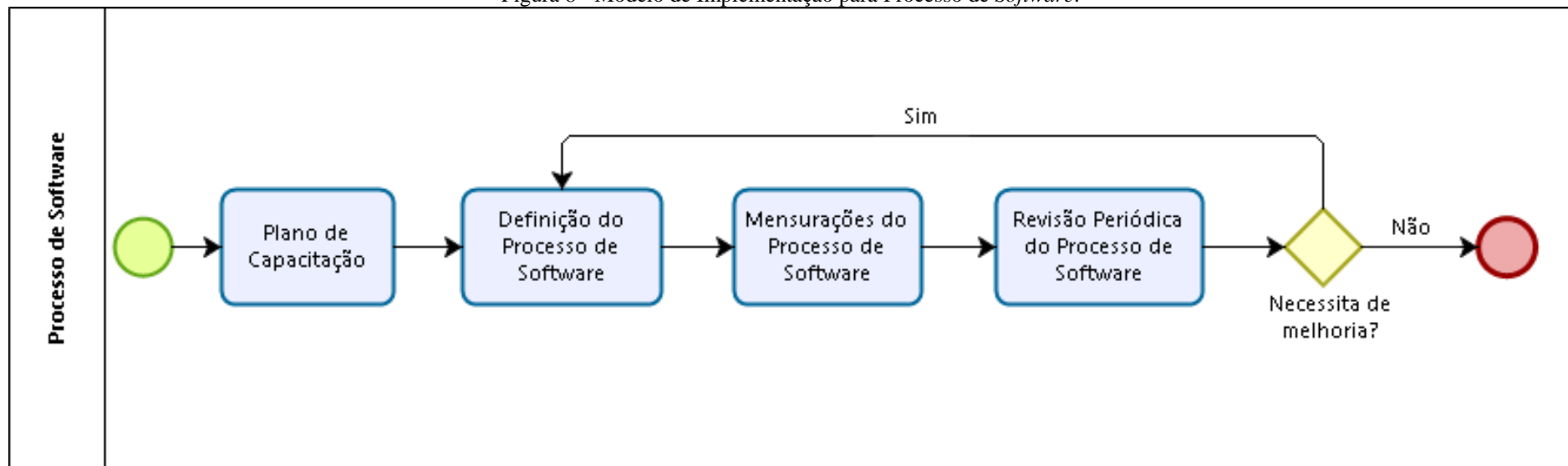


Fonte: Os Autores, 2017.

5.5 PROCESSO DE *SOFTWARE*

Esta temática está relacionada ao Processo de *Software*, com o objetivo de garantir a qualidade do produto e assegurar que ele atenda às necessidades do cliente conforme consta no contrato. Ela propõe a organização possua um processo de *software* implementado que esteja em melhoria contínua e que realize revisões conjuntas, auditorias, verificações e validações. Ela orienta também que a organização ofereça treinamentos para a equipe de desenvolvimento. A boa prática que foi utilizada para elaborar o modelo BPM apresentado na Figura 8 é a NBR ISO/IEC 12207.

Figura 8 - Modelo de Implementação para Processo de *Software*.

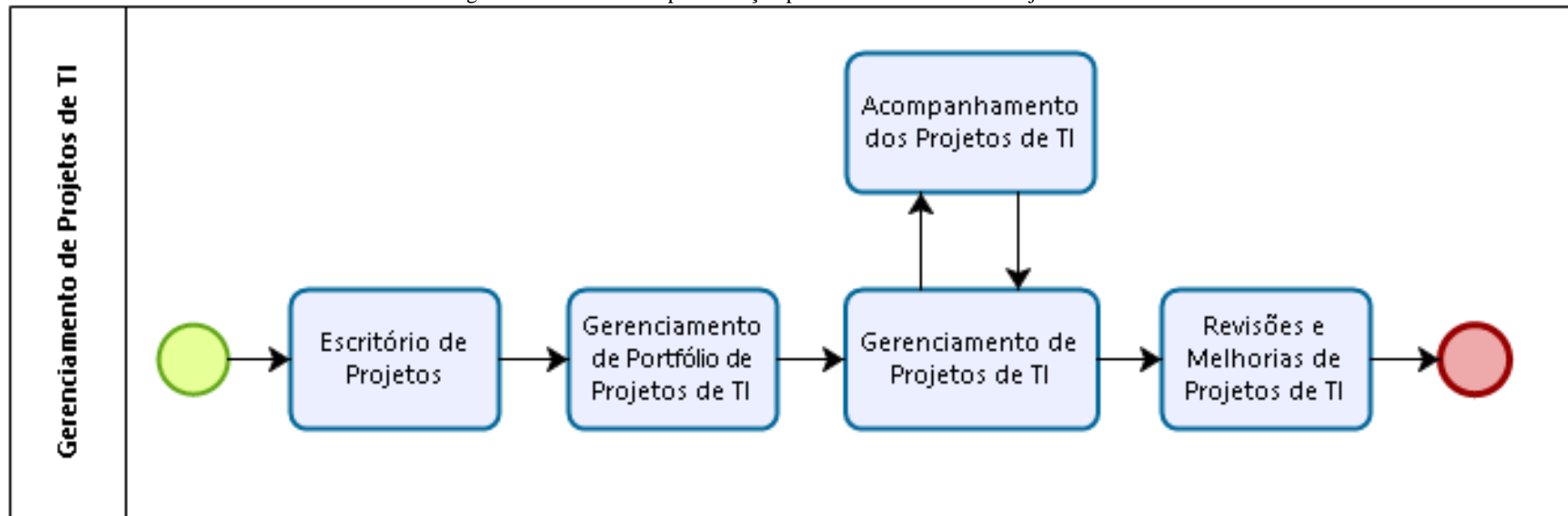


Fonte: Os Autores, 2017.

5.6 GERENCIAMENTO DE PROJETOS DE TI

Esta temática está relacionada ao Gerenciamento de Projetos de TI, com o objetivo de tornar possível o entendimento comum do projeto, permitir a troca de informações entre os projetos e possibilitar um melhor controle do ciclo de vida dos projetos. Para tal ela propõe que a organização execute um processo de Gerenciamento de Portfólio de Projetos de TI e configure um escritório de projetos. Orienta também que a organização realize um processo de Gerenciamento de Projetos de TI e acompanhe os resultados dos projetos e realize revisões de melhoria dos seus processos. As boas práticas que foram utilizadas para elaborar o modelo BPM apresentado na Figura 9 são o COBIT 5 e o PMBOK.

Figura 9 - Modelo de Implementação para Gerenciamento de Projetos de TI.

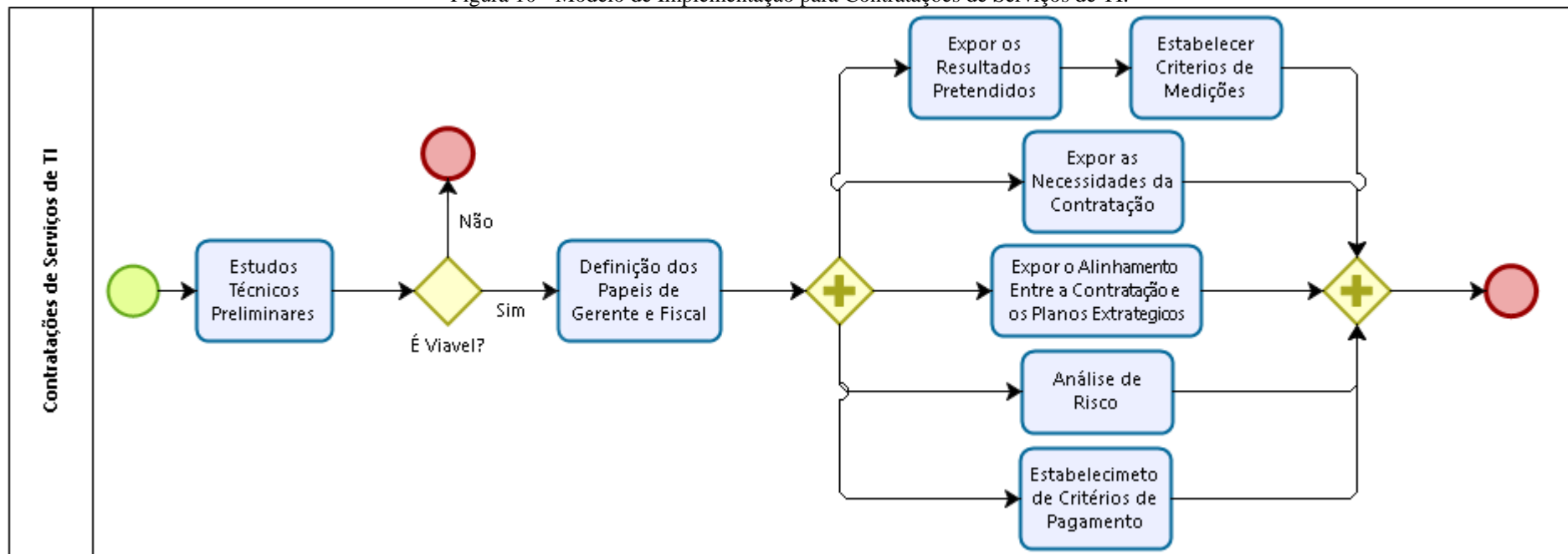


Fonte: Os Autores, 2017.

5.7 CONTRATAÇÕES DE SERVIÇOS DE TI

Esta temática está relacionada à Contratações de Serviços de TI, com o objetivo de assegurar a viabilidade técnica da contratação do serviço ou produtos de TI. Para tal ela propõe que sejam realizados estudos técnicos preliminares, análise de risco, defina os papéis de gerente e fiscal e estabeleça os critérios de pagamento. Ela orienta que no contrato conste os resultados esperados pela organização e estabeleça os critérios de medições. A boa prática utilizada para elaborar o modelo BPM apresentado na Figura 10 é o Guia de Boas Práticas em Contratação de Soluções de TI.

Figura 10 - Modelo de Implementação para Contratações de Serviços de TI.

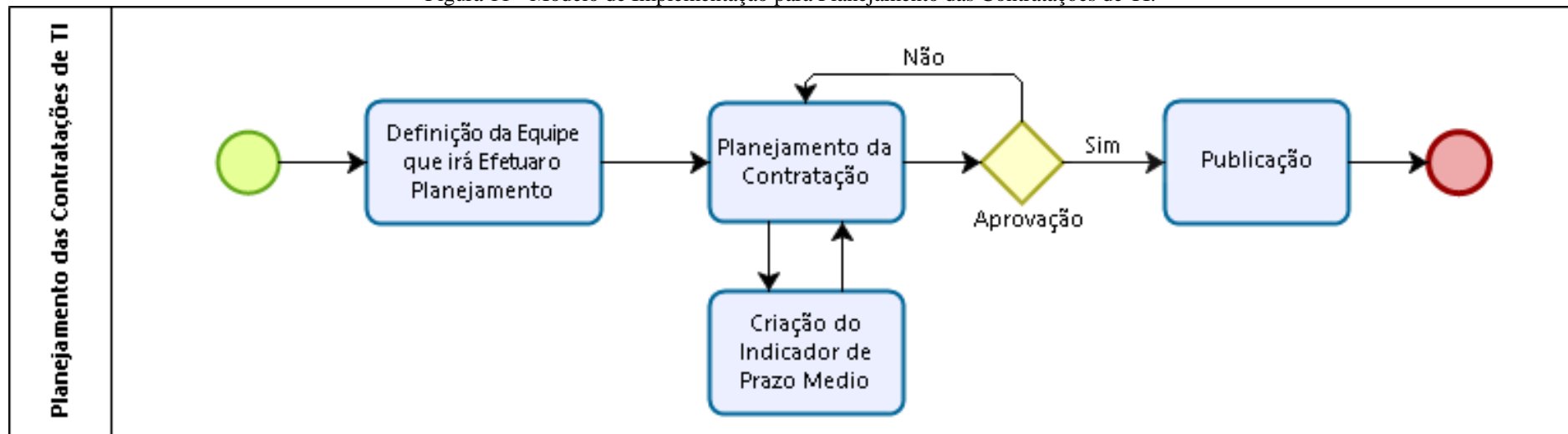


Fonte: Os Autores, 2017.

5.8 PLANEJAMENTO DAS CONTRATAÇÕES DE TI

Esta temática está relacionada ao Planejamento das Contratações de TI, com o objetivo de criar um processo padronizado para contratações e que o mesmo possa ser aprimorado continuamente. Para tal ela propõe que sejam alocados servidores capacitados e com conhecimento técnico na área da aquisição para realizar as contratações e a criação de um indicador de prazo médio para auxiliar na definição dos prazos em futuras contratações. Ela orienta também que todos os processos do planejamento sejam documentados e publicados após a aprovação pela alta administração. A boa prática utilizada para elaborar o modelo BPM apresentado na Figura 11 é o Guia de Boas Práticas em Contratação de Soluções de TI.

Figura 11 - Modelo de Implementação para Planejamento das Contratações de TI.

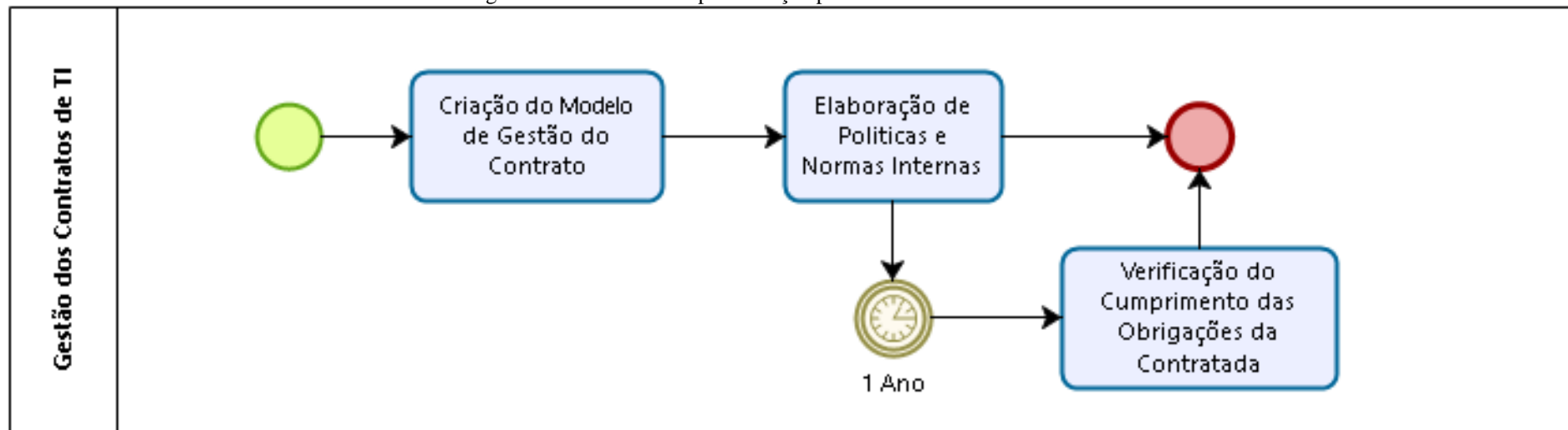


Fonte: Os Autores, 2017.

5.9 GESTÃO DOS CONTRATOS DE TI

Esta temática está relacionada à Gestão dos Contratos de TI, com o objetivo de formalizar, aprimorar e reproduzir o processo de gestão dos contratos de forma independente do servidor envolvido. Para tal ela orienta que a organização defina os critérios de qualidade, verificação e avaliação do cumprimento das obrigações da contratada e a elaboração de políticas e normas internas referentes à gestão dos contratos. A boa prática utilizada para elaborar o modelo BPM apresentado na Figura 12 é o Guia de Boas Práticas em Contratação de Soluções de TI.

Figura 12 - Modelo de Implementação para Gestão dos Contratos de TI.



Fonte: Os Autores, 2017.

6 RESULTADOS DO QUESTIONÁRIO DE VALIDAÇÃO E VERIFICAÇÃO

Nesta seção é apresentado os resultados obtidos com a aplicação do questionário, conforme Apêndice B. Foram enviados um total de cento e quarenta e quatro e-mails com uma carta convite, conforme Apêndice A, a gestores ou servidos da APF, entretanto, apenas 8 respostas foram registradas no período de 22 de setembro de 2017 há 29 de setembro de 2017.

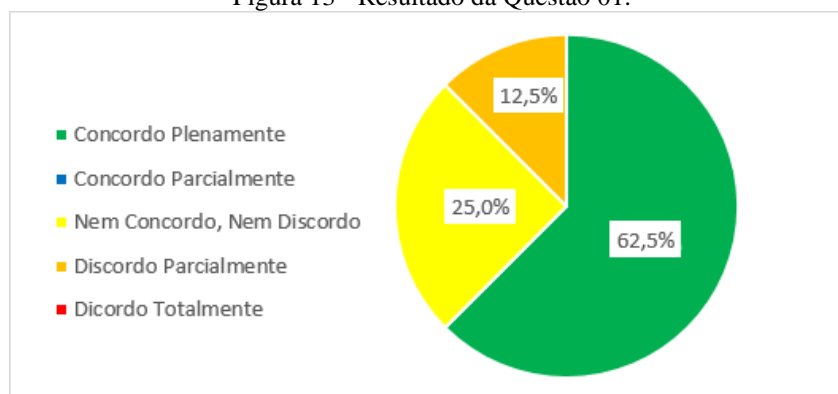
Na seção 3.1 é apresentado os resultados obtidos para avaliação dos modelos BPM, dispostos Capítulo 5. E na seção 6.2 é apresentado os resultados obtidos para validar a análise das boas práticas de GovTIC, disposta no Capítulo 4.

6.1 RESULTADO DA SEÇÃO 1: MODELOS BPM

Esta seção apresenta os resultados obtidos referente aos modelos BPM. Vale destacar que as questões que obtiveram os mesmos resultados foram agrupadas, com exceção do modelo de visão geral por englobar todos os outros modelos.

Conforme observado na Figura 13, a maioria dos respondentes avaliaram positivamente (62,5%), 25% mantiveram-se neutros e houve uma pequena discordância (12,5%) do modelo BPM da Questão 01, conforme Apêndice B. Podemos então afirmar que o modelo de visão geral poderia ser adotado em organizações da APF, de modo a auxiliar o gestor na melhoria da maturidade do iGovTI na dimensão de Processo, apesar de 1/4 dos respondentes não se posicionarem a favor, o que pode ser considerado uma alta abstenção.

Figura 13 - Resultado da Questão 01.

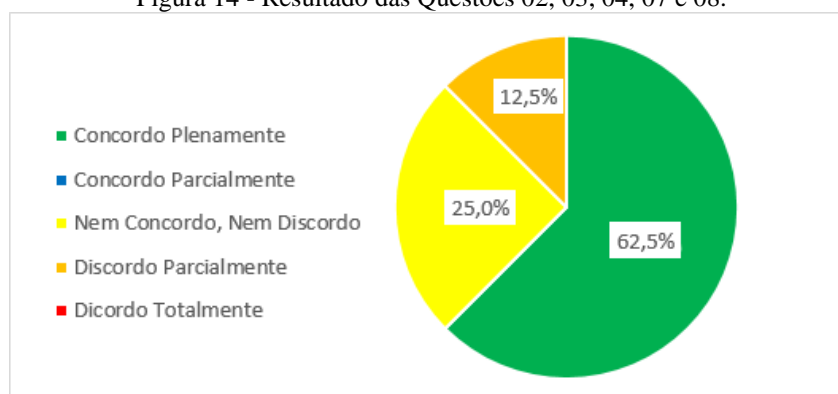


Fonte: Os Autores, 2017.

Conforme observado na Figura 14, a maioria dos respondentes a avaliaram positivamente (62,5%), 25% mantiveram-se neutros e houve uma pequena discordância

(12,5%) dos modelos BPM propostos nas Questões 02, 03, 04, 07 e 08, conforme o Apêndice B. Podemos então afirmar que o modelo poderia ser adotado em organizações da APF de modo a auxiliar o gestor na melhoria da maturidade do iGovTI para o Gerenciamento de Serviços de TI, Gerenciamento de Nível de Serviço, Gestão de Risco de TI, Gerenciamento de Projetos de TI e Contratações em Serviços de TI, apesar de 1/4 dos respondentes não se posicionarem a favor, o que pode ser considerado um alto valor de abstenção.

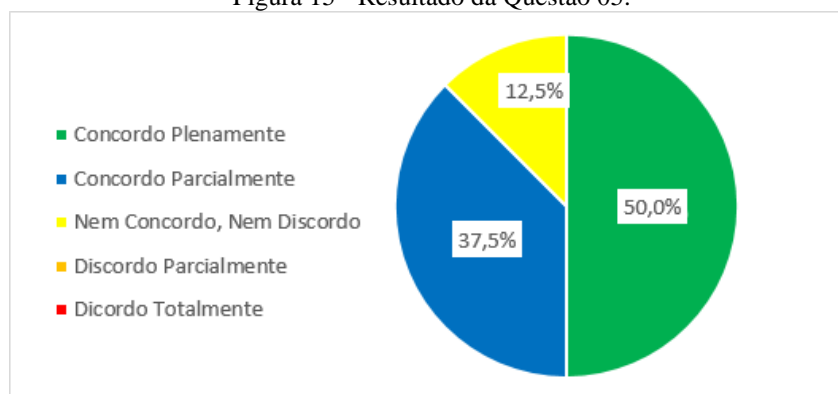
Figura 14 - Resultado das Questões 02, 03, 04, 07 e 08.



Fonte: Os Autores, 2017.

Conforme observado na Figura 15, a maioria dos respondentes a avaliaram positivamente (87,5%) e 12,5% mantiveram-se neutros em relação ao modelo BPM proposto na Questão 05, conforme o Apêndice B. Podemos então afirmar que o modelo poderia ser adotado em organizações da APF de modo a auxiliar o gestor na melhoria da maturidade do iGovTI para o Gestão Corporativa da Segurança da Informação, apesar que 37,5% dos respondentes concordarem parcialmente com o modelo proposto. Sendo importante destacar que não houveram respostas negativas.

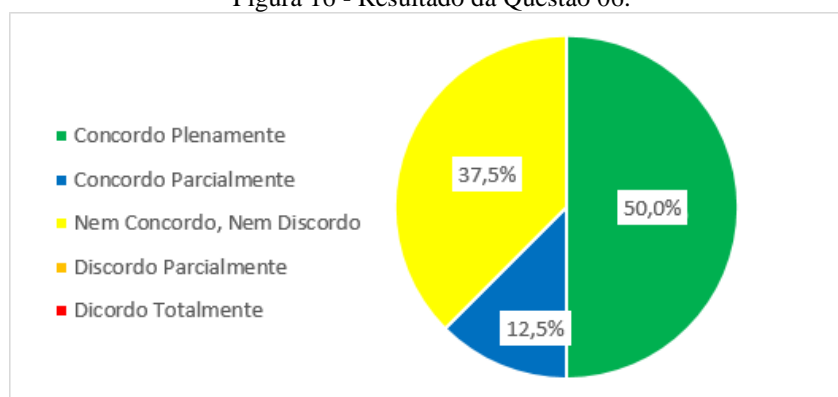
Figura 15 - Resultado da Questão 05.



Fonte: Os Autores, 2017.

Conforme observado na Figura 16, a maioria dos respondentes a avaliaram positivamente (62,5%) e 37,5% mantiveram-se neutros em relação ao modelo BPM proposto na Questão 06, conforme o Apêndice B. Podemos então afirmar que o modelo poderia ser adotado em organizações da APF de modo a auxiliar o gestor na melhoria da maturidade do iGovTI para o Processo de *Software*, apesar que 12,5% dos respondentes concordarem parcialmente e quase metade dos respondentes mantiveram-se neutros, o que pode ser considerado um alto valor de abstenção. Sendo importante destacar que não houveram respostas negativas.

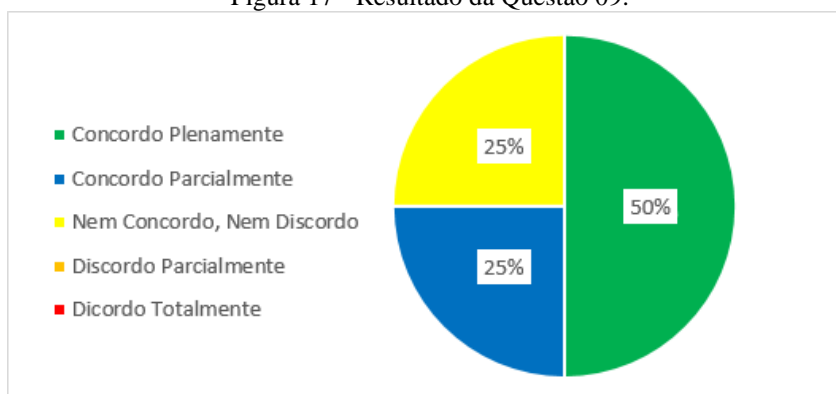
Figura 16 - Resultado da Questão 06.



Fonte: Os Autores, 2017.

Conforme observado na Figura 17, a maioria dos respondentes a avaliaram positivamente (75%) e 25% mantiveram-se neutros em relação ao modelo BPM proposto na Questão 09, conforme o Apêndice B. Podemos então afirmar que o modelo poderia ser adotado em organizações da APF de modo a auxiliar o gestor na melhoria da maturidade do iGovTI para o Planejamento das Contratações de TI, apesar que 25% dos respondentes concordarem parcialmente e 1/4 dos respondentes não se posicionarem a favor, o que pode ser considerado um alto valor de abstenção. Sendo importante destacar que não houveram respostas negativas.

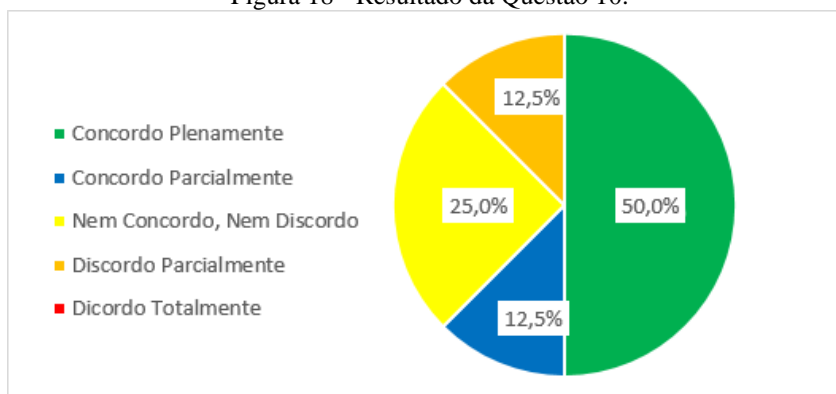
Figura 17 - Resultado da Questão 09.



Fonte: Os Autores, 2017.

Conforme observado na Figura 18, a maioria dos respondentes a avaliaram positivamente (62,5%), 25% mantiveram-se neutros e houve uma pequena discordância (12,5%) em relação ao modelo BPM proposto na Questão 10, conforme o Apêndice B. Podemos então afirmar que o modelo poderia ser adotado em organizações da APF de modo a auxiliar o gestor na melhoria da maturidade do iGovTI para a Gestão dos Contratos de TI, apesar que 12,5% dos respondentes concordarem parcialmente e 1/4 dos respondentes não se posicionarem a favor, o que pode ser considerado um alto valor de abstenção.

Figura 18 - Resultado da Questão 10.



Fonte: Os Autores, 2017.

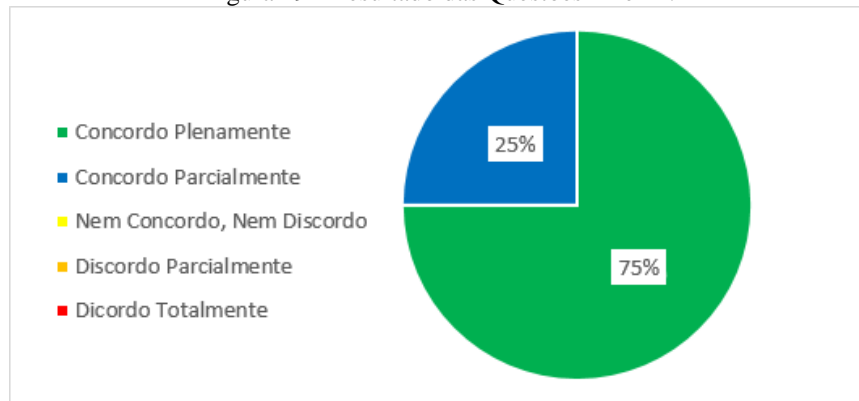
6.2 RESULTADO DA SEÇÃO 2: ANÁLISE DAS BOAS PRÁTICAS

Está seção apresenta os resultados obtidos referente a análise das boas práticas de GovTIC. Vale ressaltar que eles foram agrupados para as questões que obtiveram os mesmos resultados.

Conforme observado na Figura 19, todos os respondentes avaliaram positivamente as Questões 11 e 12. Podemos então afirmar que a apresentação de um documento que possua as

boas práticas ITIL e da NBR ISO/IEC 20000-2 de forma resumida pode auxiliar a aprimorar a maturidade do iGovTI nas temáticas Gerenciamento de Serviços de TI e Gerenciamento de Nível de Serviço de TI. E importante destacar que 25% dos respondentes concordaram parcialmente e que não houveram respostas negativas.

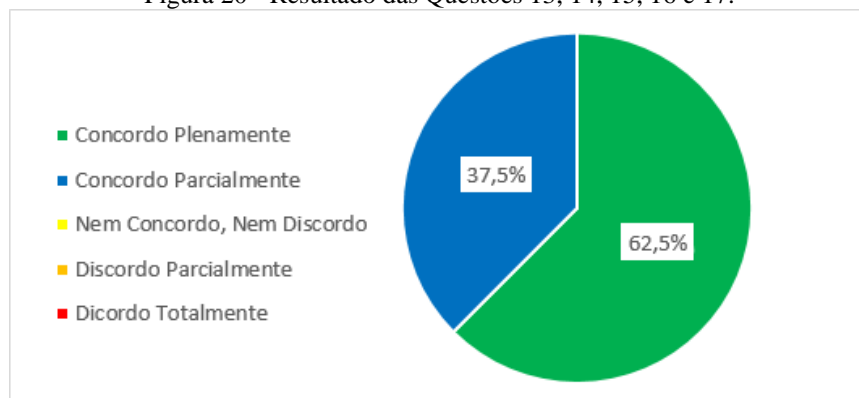
Figura 19 - Resultado das Questões 11 e 12.



Fonte: Os Autores, 2017.

Conforme observado na Figura 20, todos os respondentes avaliaram positivamente as Questões 13, 14, 15, 16 e 17. Podemos então afirmar apresentação de um documento que possua as boas práticas COBIT 5, NBR ISO 31000, NBR ISO/IEC 38500, 27001, 27002, 27005, 12207, PMBOK e o Guia de Boas Práticas em Contratação de Soluções de TI de forma resumida pode auxiliar a aprimorar a maturidade do iGovTI nas temáticas Gestão de Risco de TI, Gestão Corporativa da Segurança da Informação, Processo de *Software*, Gerenciamento de Projetos de TI, Contratações de Serviços de TI, Planejamento das Contratações de TI e Gestão dos Contratos de TI. E importante destacar que 25% dos respondentes concordaram parcialmente e que não houveram respostas negativas.

Figura 20 - Resultado das Questões 13, 14, 15, 16 e 17.



Fonte: Os Autores, 2017.

7 CONCLUSÃO

Neste trabalho foi realizada a análise de algumas das boas práticas voltadas para GovTIC com o objetivo de melhoria da maturidade do iGovTI na dimensão de Processos. Por meio da análise das boas práticas identificadas foi elaborado e são apresentados modelos BPM para auxiliar os gestores de organizações pertencentes à APF na implementação das práticas da dimensão de Processos.

Foi possível identificar que o envolvimento da alta administração é um fator que impacta diretamente na adoção das boas práticas de GovTIC, visto que a mesma fornece os mecanismos que permitem sua implementação. Em alguns momentos é necessário que ela participe ativamente realizando análises críticas e aprove ou não os aspectos de implementação das boas práticas.

Este trabalho possui como diferencial a apresentação de forma resumida e simplificada de como os gestores podem incentivar a adoção de práticas de GovTIC em sua organização, com base nas orientações que compõe o COBIT 5, o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação, a ITIL, a NBR ISO 31000, as NBR ISO/IEC 12207, 27001, 27002, 27005 e 38500 e o PMBOK, com o objetivo de melhoria da maturidade do iGovTI da organização na dimensão de Processos.

Os resultados obtidos no questionário podem ser considerados satisfatórios, sendo em a maioria das respostas foram positivas e a ocorrência de respostas negativas foram mínimas, o que valida os modelos BPM e a análise das boas práticas identificadas para melhoria da maturidade do iGovTI na dimensão de Processos.

Podemos complementar que o objetivo deste trabalho foi alcançado, visto que o objetivo geral e específicos foram atendidos, mediante a identificação das boas práticas de GovTIC que devem ser adotadas em organizações públicas (Capítulo 4), criação dos processos de implementação por meio de BPM (Capítulo 5) e realização do estudo de caso em organizações que fazem parte da APF (Capítulo 6).

Vale ressaltar que as boas práticas identificadas e analisadas no presente trabalho podem ser utilizadas pelos gestores como um documento auxiliar para implementação das mesmas, entretanto, sua aplicação não garante que esse objetivo seja alcançado ou que outras práticas aqui não listadas, não possam ser utilizadas com a mesma finalidade. Também não exclui a necessidade de consultar as boas práticas na íntegra durante sua implementação.

7.1 DIFICULDADES E AMEAÇAS A VALIDADE

Durante o desenvolvimento deste trabalho nos deparamos com algumas dificuldades e limitações. Não foi possível analisar algumas boas práticas reconhecidas na academia e na indústria de GovTIC por não ter acesso ao material das mesmas, sendo elas: COSO, CMMI, MPS.BR, NBR ISO/IEC 15504, entre outras.

Podemos citar como ameaça a validade desse trabalho, a aplicação do questionário via formulário web, não podendo afirmar que necessariamente um gestor ou servidor ligado a GovTIC como respondente. Além do baixo número de respostas recebidas, que ocasiona na avaliação de uma pequena amostra das organizações, podendo não refletir a realidade de todas. E que ocorreram um número considerável de respostas neutras aproximadamente 25% para os modelos BPM, o que torna necessário realizar uma verificação dos motivos da abstenção e se devem ser realizadas melhorias nos modelos BPM.

7.2 TRABALHOS FUTUROS

Nesta seção indicaremos trabalhos futuros que podem ser desenvolvidos para complementar ou auxiliar a aplicabilidade deste trabalho. São eles:

- a) Desenvolver uma ferramenta de acompanhamento da implementação da GovTIC;
- b) Expandir a análise e implementar o modelo BPM para as demais dimensões definidas pelo TCU, sendo elas: Liderança da Alta Administração, Estratégias e Planos, Informações, Pessoas e Resultados de TI;
- c) Identificar quais os fatores ou motivos levam as organizações a não priorizar a GovTIC; e
- d) Identificar quais os impactos da não adoção das boas práticas de GovTIC.

7.3 CONTRIBUIÇÕES AO TRABALHO

Nesta seção indicamos artigo aprovado, sendo ele: *Governance Practices of ICT in the Federal Public Administration for Risk Management in the Process Dimension* – VI Simpósio Brasileiro de Tecnologia da Informação - SBTI 2017, conforme Anexo A.

REFERÊNCIAS BIBLIOGRÁFICAS

- ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos**. Rio de Janeiro - RJ, 2006.
- ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 15504-1: Tecnologia da informação - Avaliação de processo - Parte 1: Conceitos e vocabulário**. 2008.
- ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31000: Gestão de riscos - Princípios e diretrizes**. Rio de Janeiro - RJ, 2009a.
- ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 12207: Tecnologia de Informação – Processos de ciclo de vida de software**. Rio de Janeiro - RJ, 2009b.
- ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 38500: Governança corporativa de tecnologia da informação**. Rio de Janeiro - RJ, 2009c.
- ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005: Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação**. Rio de Janeiro - RJ, 2011.
- ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 20000-2: Tecnologia da informação - Gerenciamento de serviços - Parte 2: Guia de aplicação do sistema de gestão de serviços**. Rio de Janeiro - RJ, 2013a.
- ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro - RJ, 2013b.
- ARAUJO, R. et al. **A Definição de Processos de Software sob o ponto de vista da Gestão de Processos de Negócio**. Simpósio Internacional De Melhoria De Processos De Software, v. 6, p. 23–32, 2004.
- BIZERRA, A. L. V.; ALVES, F. J. D. S.; RIBEIRO, C. D. M. D. A. **Governança pública: uma proposta de conteúdo mínimo para os relatórios de gestão das entidades governamentais**. EnAPG - Encontro de Administração Pública e Governo, p. 1–16, 2012.
- BRASIL. **Decreto nº 7579**, 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Decreto/D7579.htm>. Acesso em: 21 dez. 2016
- BRASIL. **SISP - Sistema de Administração dos Recursos de Tecnologia da Informação — Governo Eletrônico**. 2013. Disponível em: <<https://www.governoeletronico.gov.br/eixos-de-atuacao/governo/sistema-de-administracao-dos-recursos-de-tecnologia-da-informacao-sisp>>. Acesso em: 20 dez. 2016.
- BRASIL. **Governança Pública: Referencial Básico de Governança Aplicável a Órgãos e**

Entidades da Administração Pública e Ações Indutoras de Melhoria / Tribunal de Contas da União. Brasília, 2014.

BRASIL. **Administração dos Recursos de TI (SISP) — Ministério do Planejamento, Desenvolvimento e Gestão.** 2015a. Disponível em: <http://www.planejamento.gov.br/assuntos/tecnologia-da-informacao/sites-coordenados/copy_of_portal-sisp>. Acesso em: 29 jan. 2017.

BRASIL. **Apresentação — Ministério do Planejamento, Desenvolvimento e Gestão.** 2015b. Disponível em: <www.planejamento.gov.br/assuntos/logistica-e-tecnologia-da-informacao/coordenacao>. Acesso em: 29 jun. 2017.

BRASIL. **Diário Oficial da União - Portaria Nº 68 - Ministério do Planejamento, Orçamento e Gestão.** 2016a.

BRASIL. **Decreto nº 8638.** 2016b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8638.htm>. Acesso em: 4 fev. 2017.

BRASIL. **Gestão de TI: governo publica Estratégia de Governança Digital — Ministério do Planejamento, Desenvolvimento e Gestão.** 2016c. Disponível em: <<http://www.planejamento.gov.br/assuntos/logistica-e-tecnologia-da-informacao/noticias/gestao-de-ti-governo-publica-estrategia-de-governanca-digital>>. Acesso em: 4 fev. 2017.

BRASIL, Ministério do Planejamento, Orçamento e Gestão. **EGD - Estratégia de Governança Digital da Administração Pública Federal 2016-19 / Ministério do Planejamento, Orçamento e Gestão, Secretaria de Tecnologia da Informação.** Brasília, 2016d .

CHIARI, R. **O que é COBIT? Compreenda os principais conceitos do framework.** 2016. Disponível em: <<https://www.itsmnapratica.com.br/compreendendo-conceitos-cobit/>>. Acesso em: 17 jul. 2017.

COSO. **COSO: Controle Interno - Estrutura Integrada.** 2013.

ERNAWATI, T. .; SUHARDIB; NUGROHO, D. R. . **IT risk management framework based on ISO 31000:2009.** Proceedings of the 2012 International Conference on System Engineering and Technology, ICSET, 2012.

FERNANDES, A. A.; ABREU, V. F. DE. **Implantando a Governança de TI da Estratégia à Gestão dos Processos e Serviços.** 4ª ed. Brasport Livros e Multimídia Ltda, 2014.

FERREIRA, L. M.; JONES, G. D. C. **Adoção das Boas Práticas Sugeridas pela Itil no Processo de Gerenciamento de Mudança: um Instrumento de Planejamento e Controle em uma Empresa de Ti.** XI SEGeT 2014 - Simpósio de Excelência em Gestão e Tecnologia. Resende - RJ, 2014.

FONTELLES, M. J. et al. **Metodologia Da Pesquisa Científica: Diretrizes Para a Elaboração De Um Protocolo De Pesquisa.** Revista Paraense de Medicina, v. 23, n. 2, p.

1–8, 2009.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo, 2002.

HAMID, Z. A.; SULAIMAN, H. **Cobit Benchmarking Of System Development Governance For A Government Agency In Malaysia**. Journal Of Theoretical And Applied Information Technology, p. 10, 2016.

HECKERT, C. R.; AGUIAR, E. L. DE. **GOVERNANÇA DIGITAL NA ADMINISTRAÇÃO PÚBLICA FEDERAL: UMA ABORDAGEM ESTRATÉGICA PARA TORNAR O GOVERNO DIGITAL MAIS EFETIVO E COLABORATIVO - A ÓTICA DA SOCIEDADE**. IX Congresso CONSAD de Gestão Publica. Distrito Federal - Brasília, 2016.

IBGC. **Código das Melhores Práticas de Governança Corporativa**. São Paulo - SP, 2015.

IFC, INTERNATIONAL FINANCE CORPORATION. **Guia Prático de Governança Corporativa: Experiências do Círculo de Companhias da América Latina**. Pennsylvania Ave., NW, Washington, DC, 2009.

ISACA. **COBIT 5: Governança e Gestão de TI da Organização**. 2012.

ISO, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary**. 2014.

ITGI. **IT Governance Institute (ITGI)**. 2014. Disponível em: <<http://www.isaca.org/About-ISACA/IT-Governance-Institute/Pages/default.aspx>>. Acesso em: 18 set. 2017.

KOSCIANSKI, A.; SOARES, M. DOS S. **Qualidade de software: aprenda as metodologias e técnicas mais modernas para o desenvolvimento de software**. 2. ed. São Paulo: Novatec Editora, 2007.

LINCZUK, L. M. W. **Governança aplicada à administração pública – A contribuição da auditoria interna para sua efetivação: um estudo em universidades públicas federais**. p. 181, 2012.

LOUREIRO, L. DE C.; PENHA, T. DE A.; NASCIMENTO, J. M. M. DO. **Relacionamento das melhores práticas do Cobit e ITIL para a Governança de TIIX SEGeT 2012 - Simpósio de Excelência em Gestão e Tecnologia**. Resende - RJ, 2012.

MAGALHÃES, I. L.; PINHEIRO, W. B. **Gerenciamento de Serviços de TI na Prática: Uma abordagem com base na ITIL**. p. 672, 2007.

MALHOTRA, N. K. **Pesquisa de Marketing: uma orientação aplicada**. 3º ed. Porto Alegre: Bookman, 2001.

MATIAS-PEREIRA, J. **A Governança Corporativa Aplicada No Setor Público Brasileiro**. Administração Pública e Gestão Social, v. 2, n. 1, p. 109–134, 2010.

- OLIVEIRA JÚNIOR, N. C. **Uma proposta de implantação de governança de TIC em instituições federais de ensino**. Recife, 2015.
- PETERSON, R. **Crafting information technology governance**. Information Systems Management, v. 21, n. 4, p. 7–22, 2004.
- ROUILLER, A. C. et al. **ProQualiti: Núcleo de Estudos em Engenharia e Qualidade de Software**. v. 2, 2006.
- SILVA, M. B. D. DA et al. **Public ICT Governance: a Quasi-Systematic Review**. Aracaju, 2017a.
- SILVA, M. B. D. DA et al. **Iniciativas Nacionais de Governança de TIC que sugerem Modelos, Técnicas e Boas Práticas para a Administração Pública Federal: um Mapeamento Sistemático**. v. 10, n. 1, p. 39–51, 2017b.
- SILVEIRA, D. T.; CÓRDOVA, F. P. **A pesquisa científica**. 2009.
- SOFTEX. **MPS.BR | Softex**. Disponível em: <<http://www.softex.br/mpsbr/>>. Acesso em: 20 jun. 2017.
- SOMMERVILLE, I. **Engenharia de Software**. 9ª ed. São Paulo, SP: Pearson Prentice Hal, 2011.
- TCU. **Relatório de Levantamento da Governança em Tecnologia da Informação. Grupo I - Classe V - Plenário**. Sessão Plenária, v. TC 003.732, p. 40, 2014.
- TCU. **Referências do Questionário de Governança de TI 2016**. 2016.
- TCU. **Relatório de Levantamento. Avaliação da Governança de Tecnologia da Informação na Administração Pública Federal. Grupo tagGrupo - Classe V - tagColegiado**. Sessão Plenária, TC 008.127/2016-6. 2017.
- VASCONCELLOS, F. P. **GESTÃO DE PROCESSOS DE NEGÓCIO E GOVERNANÇA DE TI: um estudo em instituições financeiras**. p. 0–46, 2012.
- VASCONCELLOS, F. P. **GESTÃO DE PROCESSOS DE NEGÓCIO E GOVERNANÇA DE TI: um modelo para avaliação do alinhamento**. Belo Horizonte, 2013.
- WEILL, P.; ROSS, J. W. **Governança de TI: Tecnologia da Informação**. São Paulo: M.Books do Brasil, 2006.
- YOSHITAKE, M. et al. **OS PILARES DA GOVERNANÇA CORPORATIVA NAS ORGANIZAÇÕES**. p. 1–13, 2014.

APÊNDICES

APÊNDICE A: E-MAIL

Título do e-mail: Carta Convite - Questionário de Governança de TIC em um estudo acadêmico.

Prezado (a) Gestor ou Servidor Público de uma Organização da APF,

O Departamento de Ciência da Computação da Universidade Federal de Sergipe está desenvolvendo um estudo acadêmico com o objetivo de identificar **“Boas Práticas de Governança de TIC Adotadas para a Melhoria do iGovTI na Administração Pública Federal na Dimensão de Processos”**.

Você está recebendo esse e-mail, pois foi identificado como parte do nosso universo de pesquisa: Gestores ou Servidores Públicos da Administração Pública Federal que lideram ou participam de trabalhos de Governança de TIC. Por isso, solicitamos a sua colaboração.

Caso queira receber os resultados da pesquisa, entre em contato com um dos envolvidos citados abaixo via e-mail. Preservaremos a privacidade dos seus dados e você não será identificado(a), já que as informações serão analisadas em termos globais.

O link da pesquisa é: <https://goo.gl/forms/nrZZV6cckS3vRIDE2> [Se o link não funcionar, copie e cole-o na caixa de endereço do seu navegador].

O questionário estará disponível online até 29 de Setembro de 2017.

Desde já expressamos os mais sinceros agradecimentos e colocamo-nos à disposição para quaisquer esclarecimentos.

Atenciosamente,

Alef Menezes dos Santos
Graduando em Sistemas de Informação – UFS
alefms@dcomp.ufs.br

Danilo Gois dos Anjos
Graduando em Sistemas de Informação – UFS
danilo.anjos@dcomp.ufs.br

Marianne Batista Diniz da Silva
Mestranda em Ciências da Computação – UFS
mariannebds@dcomp.ufs.br

Rogério Patrício C. do Nascimento
Prof. Doutor em Ciências da Computação - UFS
rogerio@ufs.br

APÊNDICE B: QUESTIONÁRIO

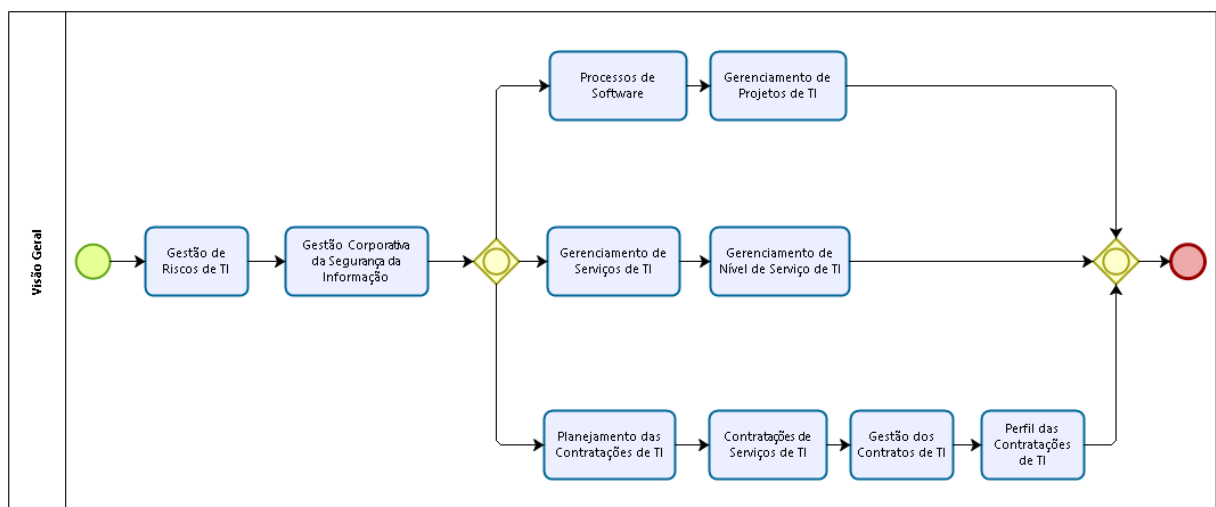
Questionário de validação das boas práticas para Dimensão de Processos

Questionário aplicado pelos alunos Alef Menezes e Danilo Gois, com objetivo de validar os modelos de processo BPM e o documento contendo as boas práticas de forma resumida para os gestores das organizações da Administração Pública Federal (APF), servindo como um estudo de caso. Essa pesquisa é parte do Trabalho de Conclusão de Curso II como parte dos requisitos para obtenção do título de Bacharel em Sistemas de Informação, com orientação do Prof. Dr. Rogério Patrício Chagas do Nascimento e coorientação da Prof(a) Marianne Batista Diniz da Silva. Todas as respostas serão analisadas de forma anônima nesta pesquisa.

Seção 1 - Modelos BPM

Esta seção está dividida em 10 questões com o intuito de validar se a apresentação de modelos de processo BPM pode auxiliar as organizações da APF na melhoria da maturidade do iGovTI.

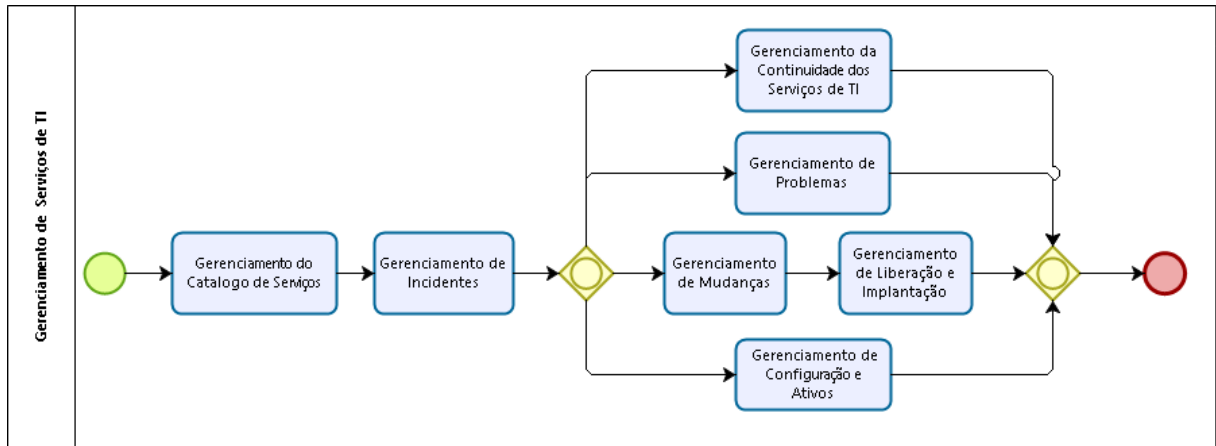
1. O modelo de visão geral abaixo pode ser aplicado para a melhoria da maturidade do iGovTI na sua organização.



Link para imagem com melhor qualidade: <https://goo.gl/kH2KQy>

- ☐ Discordo Totalmente;
- ☐ Discordo Parcialmente;
- ☐ Nem Concordo, Nem Discordo;
- ☐ Concordo Parcialmente;
- ☐ Concordo Plenamente.

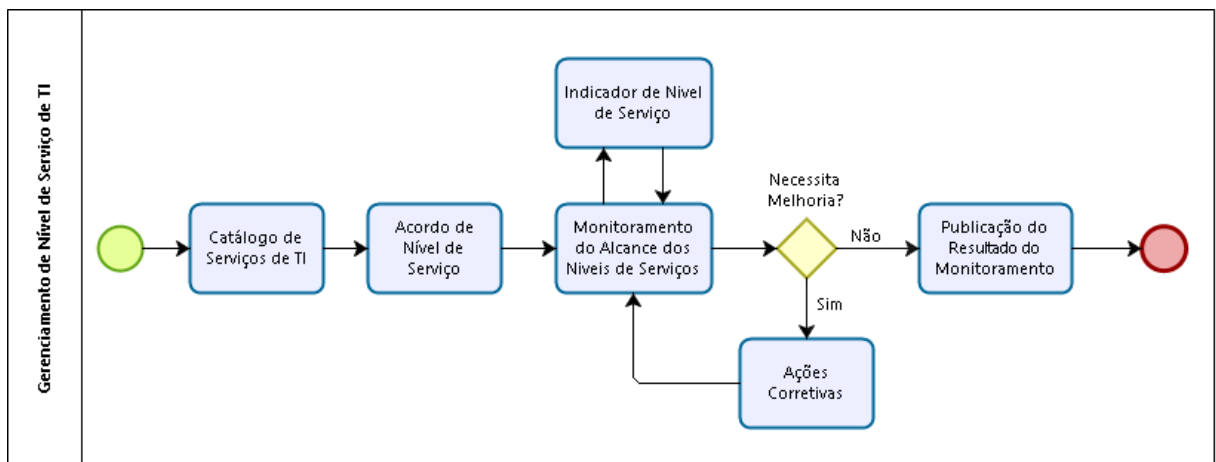
2. Gerenciamento de Serviços de TI: o modelo abaixo ao ser aplicado em sua organização auxilia o gestor de TI a catalogar os serviços executados e garantir a oferta contínua dos serviços com o mínimo de interrupção.



Link para imagem com melhor qualidade: <https://goo.gl/cSz3ug>

- ☐ Discordo Totalmente;
☐ Discordo Parcialmente;
☐ Nem Concordo, Nem Discordo;
☐ Concordo Parcialmente;
☐ Concordo Plenamente.

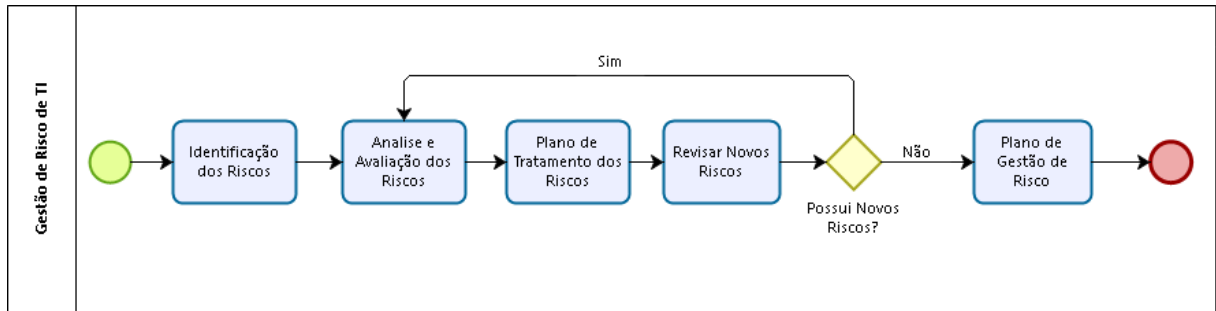
3. Gerenciamento de Nível de Serviço de TI: o modelo abaixo ao ser aplicado em sua organização auxilia o gestor de TI a acompanhar e gerenciar a entrega dos serviços executados pela organização.



Link para imagem com melhor qualidade: <https://goo.gl/nQcuhM>

- ☐ Discordo Totalmente;
☐ Discordo Parcialmente;
☐ Nem Concordo, Nem Discordo;
☐ Concordo Parcialmente;
☐ Concordo Plenamente.

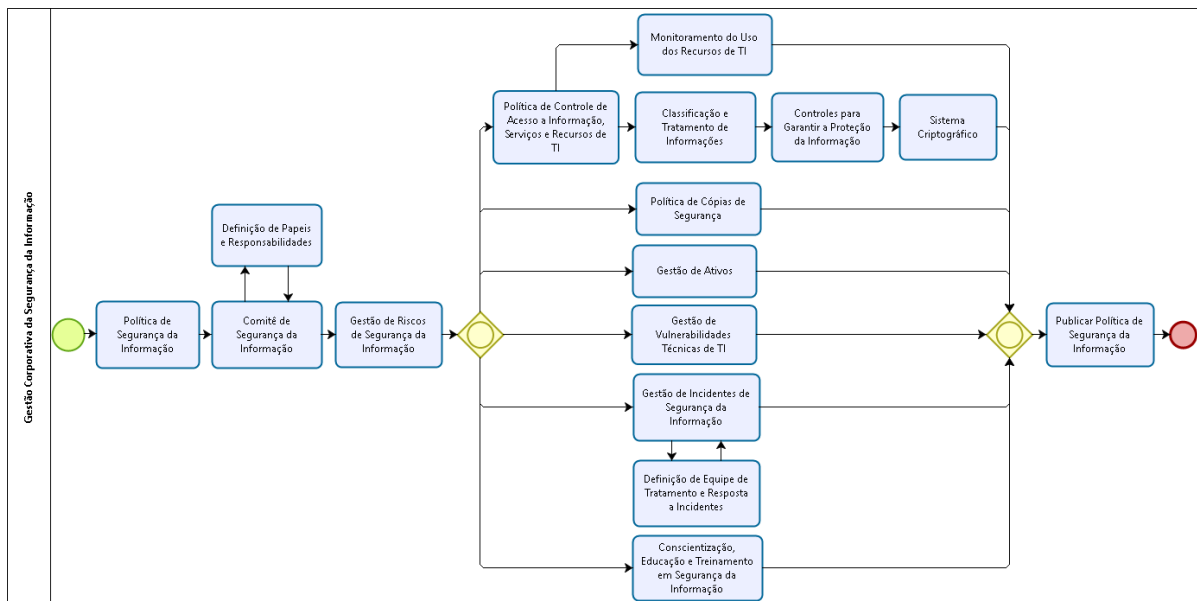
4. Gestão de Riscos de TI: o modelo abaixo ao ser aplicado em sua organização auxilia o gestor de TI a identificar, analisar, avaliar e definir o tratamento do risco, conforme sua gravidade, de modo a garantir a continuidade das atividades de TI, mitigar o risco e seu impacto na organização.



Link para imagem com melhor qualidade: <https://goo.gl/tT1PQq>

- ☐ Discordo Totalmente;
☐ Discordo Parcialmente;
☐ Nem Concordo, Nem Discordo;
☐ Concordo Parcialmente;
☐ Concordo Plenamente.

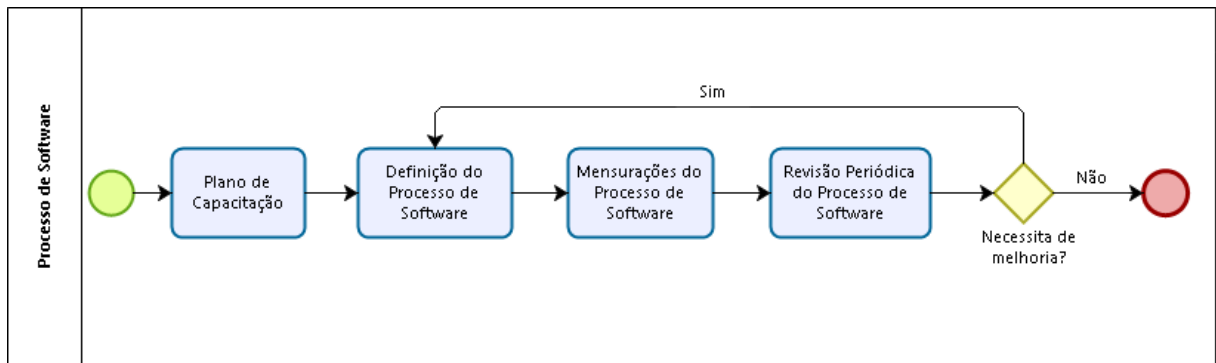
5. Gestão Corporativa da Segurança da Informação: o modelo abaixo ao ser aplicado em sua organização auxilia o gestor de TI a prevenir, identificar e determinar as ações necessárias para garantir a segurança da informação em caso de invasões ou violações.



Link para imagem com melhor qualidade: <https://goo.gl/kQRYMK>

- ☐ Discordo Totalmente;
☐ Discordo Parcialmente;
☐ Nem Concordo, Nem Discordo;
☐ Concordo Parcialmente;
☐ Concordo Plenamente.

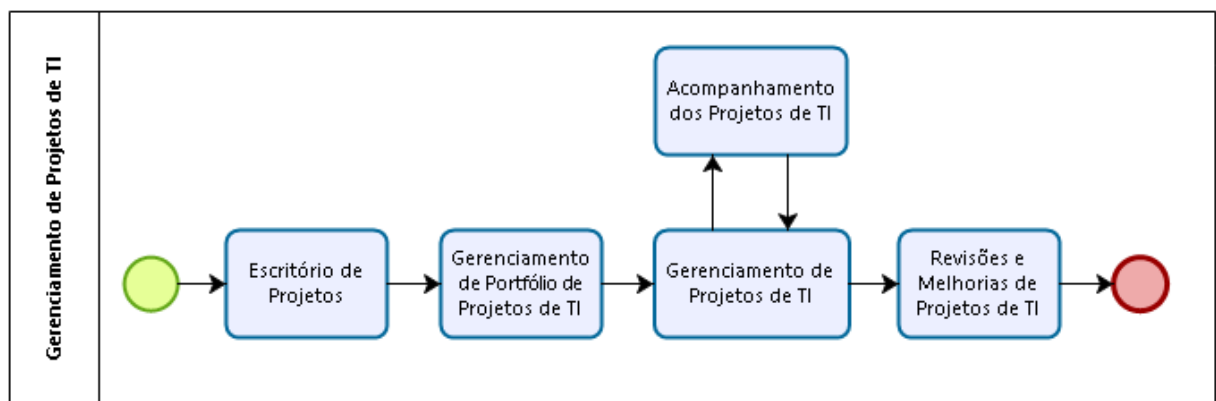
6. Processo de Software: o modelo abaixo ao ser aplicado em sua organização auxilia o gestor de TI a garantir a qualidade do produto e assegurar que ele atenda às necessidades do cliente.



Link para imagem com melhor qualidade: <https://goo.gl/BYMyN>

- ☐ Discordo Totalmente;
☐ Discordo Parcialmente;
☐ Nem Concordo, Nem Discordo;
☐ Concordo Parcialmente;
☐ Concordo Plenamente.

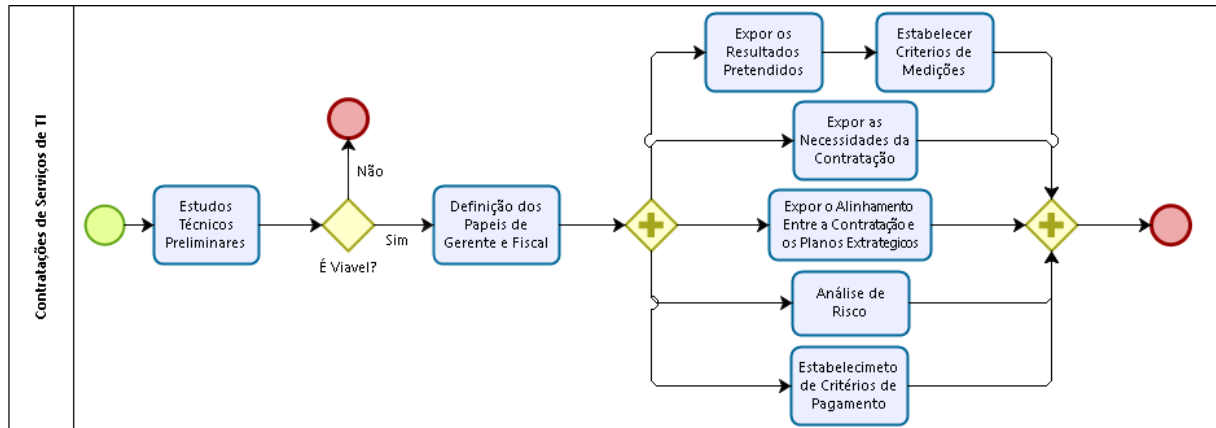
7. Gerenciamento de Projetos de TI: o modelo abaixo ao ser aplicado em sua organização auxilia o gestor de TI a tornar possível o entendimento comum do projeto, permitir a troca de informações entre projetos e possibilitar um melhor controle do ciclo de vida dos projetos.



Link para imagem com melhor qualidade: <https://goo.gl/Du6QBj>

- ☐ Discordo Totalmente;
☐ Discordo Parcialmente;
☐ Nem Concordo, Nem Discordo;
☐ Concordo Parcialmente;
☐ Concordo Plenamente.

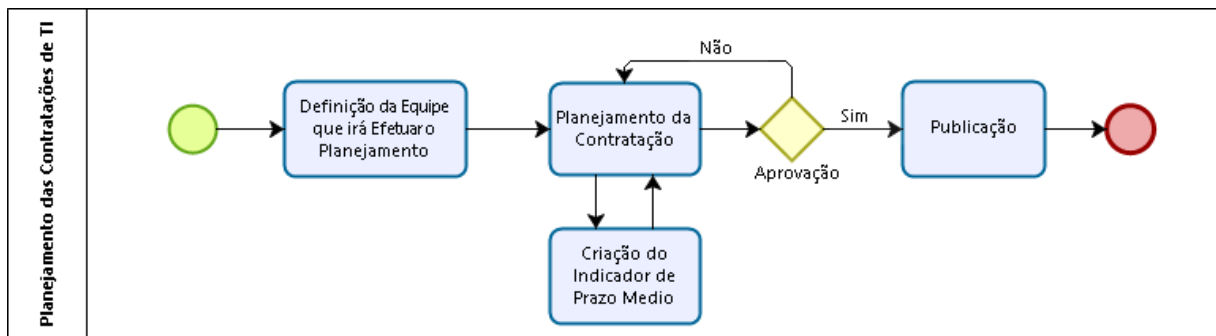
8. Contratações de Serviços de TI: o modelo abaixo ao ser aplicado em sua organização auxilia o gestor de TI a assegurar a viabilidade técnica da contratação do serviço ou produtos de TI.



Link para imagem com melhor qualidade: <https://goo.gl/y3Mgfv>

- ☐ Discordo Totalmente;
☐ Discordo Parcialmente;
☐ Nem Concordo, Nem Discordo;
☐ Concordo Parcialmente;
☐ Concordo Plenamente.

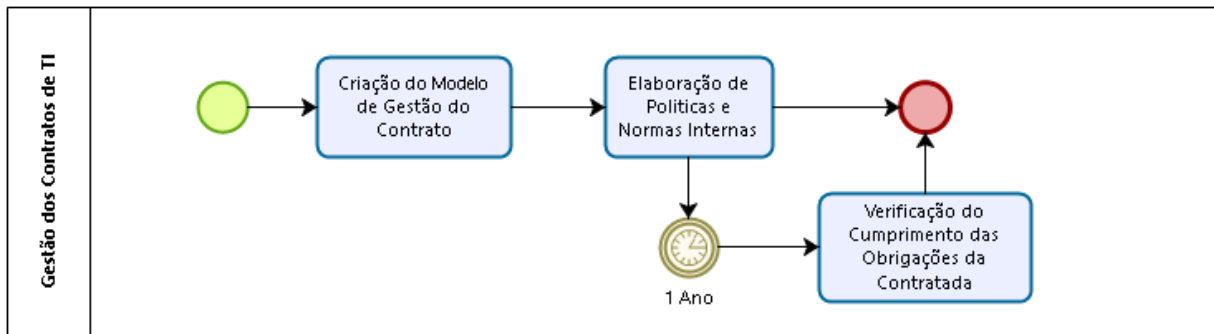
9. Planejamento das Contratações de TI: o modelo abaixo ao ser aplicado em sua organização auxilia o gestor de TI a criar um processo padronizado para contratações e que o mesmo possa ser aprimorado continuamente.



Link para imagem com melhor qualidade: <https://goo.gl/YHCFSD>

- ☐ Discordo Totalmente;
☐ Discordo Parcialmente;
☐ Nem Concordo, Nem Discordo;
☐ Concordo Parcialmente;
☐ Concordo Plenamente.

10. Referente à Gestão dos Contratos de TI, o modelo BPM ilustrado na figura abaixo ao ser aplicado na organização pode auxiliar o gestor de TI a formalizar, aprimorar e reproduzir o processo de gestão dos contratos de forma independente do servidor envolvido.



Link para imagem com melhor qualidade: <https://goo.gl/LJM6gm>

- ☐ Discordo Totalmente;
- ☐ Discordo Parcialmente;
- ☐ Nem Concordo, Nem Discordo;
- ☐ Concordo Parcialmente;
- ☐ Concordo Plenamente.

Seção 2 - Análise das Boas Práticas

Esta seção está dividida em 7 questões com o intuito de validar se a apresentação de um documento que possua boas práticas de Governança de TIC de forma RESUMIDA pode auxiliar as organizações da APF na melhoria da maturidade do iGovTI.

11. A apresentação de um documento contendo a boa prática ITIL de forma resumida auxilia os gestores de TI a aprimorar a maturidade do iGovTI na temática Gerenciamento de Serviços de TI.

- ☐ Discordo Totalmente;
- ☐ Discordo Parcialmente;
- ☐ Nem Concordo, Nem Discordo;
- ☐ Concordo Parcialmente;
- ☐ Concordo Plenamente.

12. A apresentação de um documento contendo as boas práticas ITIL e NBR ISO/IEC 20000-2 de forma resumida auxilia os gestores de TI a aprimorar a maturidade do iGovTI na temática Gerenciamento de Nível de Serviço de TI.

- ☐ Discordo Totalmente;
- ☐ Discordo Parcialmente;
- ☐ Nem Concordo, Nem Discordo;
- ☐ Concordo Parcialmente;
- ☐ Concordo Plenamente.

13. A apresentação de um documento contendo as boas práticas NBR ISO/IEC 38500, COBIT 5 e NBR ISO 31000 de forma resumida auxilia os gestores de TI a aprimorar a maturidade do iGovTI na temática Gestão de Risco de TI.

- ☐ Discordo Totalmente;
- ☐ Discordo Parcialmente;
- ☐ Nem Concordo, Nem Discordo;
- ☐ Concordo Parcialmente;

☐ Concordo Plenamente.

14. A apresentação de um documento contendo as boas práticas NBR ISO/IEC 27001, 27002 e 27005 de forma resumida auxilia os gestores de TI a aprimorar a maturidade do iGovTI na temática Gestão Corporativa da Segurança da Informação.

- ☐ Discordo Totalmente;
- ☐ Discordo Parcialmente;
- ☐ Nem Concordo, Nem Discordo;
- ☐ Concordo Parcialmente;
- ☐ Concordo Plenamente.

15. A apresentação de um documento contendo a boa prática NBR ISO/IEC 12207 de forma resumida auxilia os gestores de TI a aprimorar a maturidade do iGovTI na temática Processo de Software.

- ☐ Discordo Totalmente;
- ☐ Discordo Parcialmente;
- ☐ Nem Concordo, Nem Discordo;
- ☐ Concordo Parcialmente;
- ☐ Concordo Plenamente.

16. A apresentação de um documento contendo as boas práticas COBIT 5 e PMBOK de forma resumida auxilia os gestores de TI a aprimorar a maturidade do iGovTI na temática Gerenciamento de Projetos de TI.

- ☐ Discordo Totalmente;
- ☐ Discordo Parcialmente;
- ☐ Nem Concordo, Nem Discordo;
- ☐ Concordo Parcialmente;
- ☐ Concordo Plenamente.

17. A apresentação de um documento contendo a boa prática Guia de Boas Práticas em Contratação de Soluções de TI de forma resumida auxilia os gestores de TI a aprimorar a maturidade do iGovTI nas temáticas Contratações de Serviços de TI, Planejamento das Contratações de TI e Gestão dos Contratos de TI.

- ☐ Discordo Totalmente;
- ☐ Discordo Parcialmente;
- ☐ Nem Concordo, Nem Discordo;
- ☐ Concordo Parcialmente;
- ☐ Concordo Plenamente.

ANEXOS

ANEXO A: E-MAIL DE APROVAÇÃO DO ARTIGO



SBTI 2017 <jems@sbc.org.br>

para mim, Marianne, Danilo ▾

Prezado(a) Mr. Alef Santos:

Parabéns!!! Seu artigo "Governance Practices of ICT in the Federal Public Administration for Risk Management in the Process Dimension", submetido ao SBTI 2017, foi aceito para apresentação.

A versão final dos artigos, levando em considerações as anotações dos avaliadores deve ser reenviada até o dia 18/09. No entanto, é interessante ressaltar que os nove melhores trabalhos, se devidamente inscritos e apresentados no simpósio, serão convidados a publicação imediata na Revista Gestão.Org, avaliada pela CAPES como B2 na área de Administração Pública e de Empresas.

Por favor, note que pelo menos um dos autores do artigo - deve obrigatoriamente - se inscrever no evento, no site <https://www.faculdadeguararapes.edu.br/sbti2017/>.

Comissão Organizadora SBTI 2017 Denis Silveira e Jairo Dornelas.